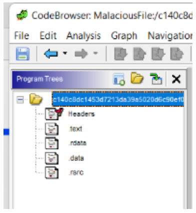
Malware Analysis Report Using Ghidra

- Trojan.GenericKD.3652107

1. What are the different segments or sections in case of each malware?

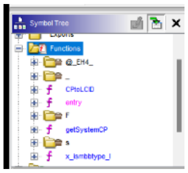
Segments section


CodeBrowser: MalaciousFile:/c140c8d
File Edit Analysis Graph Navigatior
Program Trees

c140c8dc1453d7213da39a5020d6c90e10
Headers
.text
.rdata
.data
.rsrc

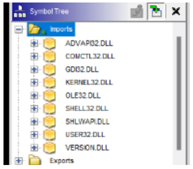
2. What are different functions, imports and exports of each Malware?

Its the functions that use by this malware.



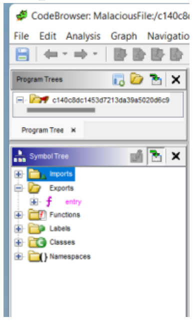
Exports
Functions
@_EH4_
_
CPtoLCID
entry
F
getSystemCP
s
x_ismbbtype_l

Imports



Imports
ADVAPI32.DLL
COMCTL32.DLL
GDI32.DLL
KERNEL32.DLL
OLE32.DLL
SHELL32.DLL
SHLWAPI.DLL
USER32.DLL
VERSION.DLL
Exports

Exports

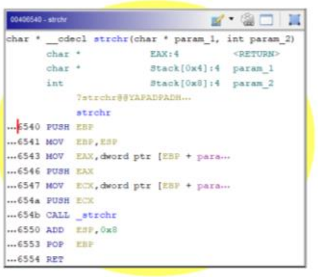

CodeBrowser: MalaciousFile:/c140c8
File Edit Analysis Graph Navigatio
Program Trees
Program Tree
Symbol Tree

c140c8dc1453d7213da39a5020d6c9
Imports
Exports
entry
Functions
Labels
Classes
Namespaces

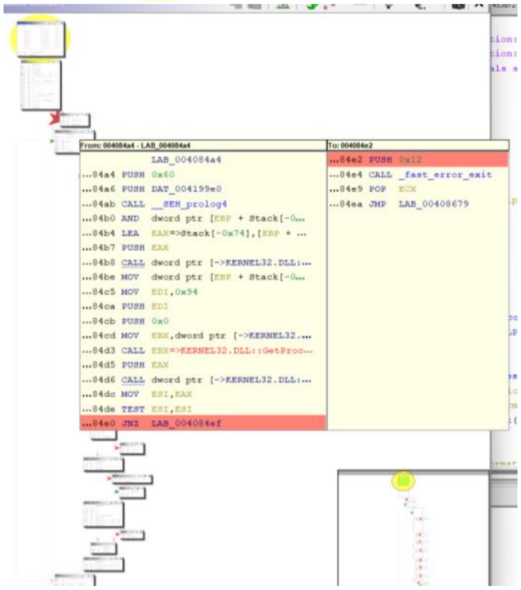
3. What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

Flow of Functions

Suspicious Functions



```
char * __cdecl strchr(char * param_1, int param_2)
        char *            EAX:4           <RETURN>
        char *            Stack[0x4]:4    param_1
        int               Stack[0x8]:4    param_2
            ?strchr@@YAPADPADH...
            strchr
...6540 PUSH EBP
...6541 MOV  EBP,ESP
...6543 MOV  EAX,dword ptr [EBP + para...
...6546 PUSH EAX
...6547 MOV  ECX,dword ptr [EBP + para...
...654a PUSH ECX
...654b CALL _strchr
...6550 ADD  ESP,0x8
...6553 POP  EBP
...6554 RET
```



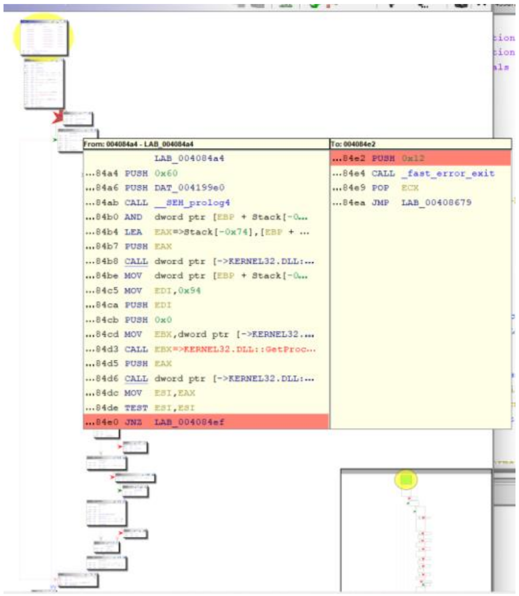
From: 004084a4 - LAB_004084a4

```
            LAB_004084a4
...84a4 PUSH DAT_004199e0
...84a6 PUSH DAT_004199e0
```

```
            LAB_004084a4
...84a4 PUSH 0x60
...84a6 PUSH DAT_004199e0
...84ab CALL __SEH_prolog4
...84b0 AND  dword ptr [EBP + Stack[-0...
...84b4 LEA  EAX=>Stack[-0x74],[EBP + ...
...84b7 PUSH EAX
...84b8 CALL dword ptr [->KERNEL32.DLL:...
...84be MOV  dword ptr [EBP + Stack[-0...
...84c5 MOV  EDI,0x94
...84ca PUSH EDI
...84cb PUSH 0x0
...84cd MOV  EBX,dword ptr [->KERNEL32....
...84d3 CALL EBX=>KERNEL32.DLL::GetProc...
...84d5 PUSH EAX
...84d6 CALL dword ptr [->KERNEL32.DLL:...
...84dc MOV  ESI,EAX
...84de TEST ESI,ESI
...84e0 JNS  LAB_004084ef
```

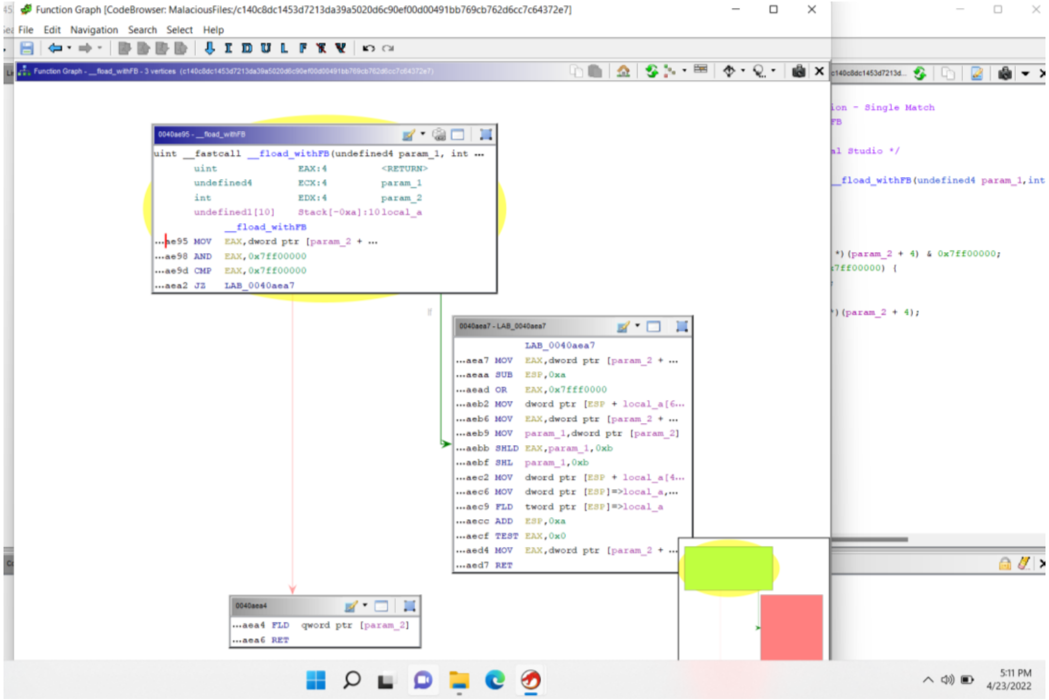
To: 004084e2

```
...84e2 PUSH 0x12
...84e4 CALL _fast_error_exit
...84e9 POP  ECX
...84ea JMP  LAB_00408679
```



```
From: 004084a4 - LAB_004084a4
                 LAB_004084a4
...84a4 PUSH     0x60
...84a6 PUSH     DAT_004199e0
...84ab CALL     __SEH_prolog4
...84b0 AND      dword ptr [EBP + Stack[-0...
...84b4 LEA      EAX=>Stack[-0x74],[EBP + ...
...84b7 PUSH     EAX
...84b8 CALL     dword ptr [->KERNEL32.DLL:...
...84be MOV      dword ptr [EBP + Stack[-0...
...84c5 MOV      EDI,0x94
...84ca PUSH     EDI
...84cb PUSH     0x0
...84cd MOV      EBX,dword ptr [->KERNEL32....
...84d3 CALL     EBX=>KERNEL32.DLL::GetProc...
...84d5 PUSH     EAX
...84d6 CALL     dword ptr [->KERNEL32.DLL:...
...84dc MOV      ESI,EAX
...84de TEST     ESI,ESI
...84e0 JNZ      LAB_004084ef
```

```
To: 004084e2
...84e2 PUSH     0x12
...84e4 CALL     _fast_error_exit
...84e9 POP      ECX
...84ea JMP      LAB_00408679
```


Function Graph [CodeBrowser: MalaciousFiles:/c140c8dc1453d7213da39a5020d6c90ef00d00491bb769cb762d6cc7c64372e7]
File Edit Navigation Search Select Help
Function Graph - __fload_withFB - 3 vertices (c140c8dc1453d7213da39a5020d6c90ef00d00491bb769cb762d6cc7c64372e7)
5:11 PM
4/23/2022

```
0040ae95 - __fload_withFB
uint __fastcall __fload_withFB(undefined4 param_1, int ...
        uint            EAX:4          <RETURN>
        undefined4      ECX:4          param_1
        int             EDX:4          param_2
        undefined1[10]  Stack[-0xa]:10 local_a
                   __fload_withFB
...ae95 MOV   EAX,dword ptr [param_2 + ...
...ae98 AND   EAX,0x7ff00000
...ae9d CMP   EAX,0x7ff00000
...aea2 JZ    LAB_0040aea7
```

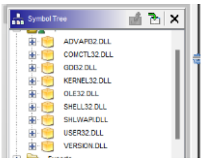
```
0040aea7 - LAB_0040aea7
                 LAB_0040aea7
...aea7 MOV   EAX,dword ptr [param_2 + ...
...aeaa SUB   ESP,0xa
...aead OR    EAX,0x7fff0000
...aeb2 MOV   dword ptr [ESP + local_a[6...
...aeb6 MOV   EAX,dword ptr [param_2 + ...
...aeb9 MOV   param_1,dword ptr [param_2]
...aebb SHLD  EAX,param_1,0xb
...aebf SHL   param_1,0xb
...aec2 MOV   dword ptr [ESP + local_a[4...
...aec6 MOV   dword ptr [ESP]=>local_a,...
...aec9 FLD   tword ptr [ESP]=>local_a
...aecc ADD   ESP,0xa
...aecf TEST  EAX,0x0
...aed4 MOV   EAX,dword ptr [param_2 + ...
...aed7 RET
```

```
0040aea4
...aea4 FLD   qword ptr [param_2]
...aea6 RET
```

```
ion - Single Match
FB
l Studio */
_fload_withFB(undefined4 param_1,int
*)(param_2 + 4) & 0x7ff00000;
7ff00000) {
*)(param_2 + 4);
```

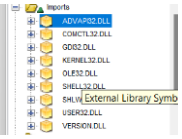
4. What DLL's any malware includes? Is there any suspicious functionality called by these DLL's?

DLL



ADVAPI32.DLL
COMCTL32.DLL
GDI32.DLL
KERNEL32.DLL
OLE32.DLL
SHELL32.DLL
SHLWAPI.DLL
USER32.DLL
VERSION.DLL

Suspicious functionality dll

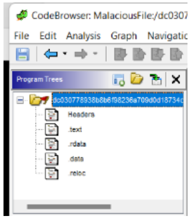


Imports
ADVAPI32.DLL
COMCTL32.DLL
GDI32.DLL
KERNEL32.DLL
OLE32.DLL
SHELL32.DLL
SHLW
USER32.DLL
VERSION.DLL

- ➢ Password-Stealer (003bbfec1)

1. What are the different segments or sections in case of each malware?

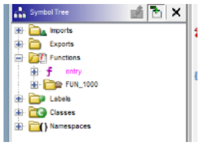
Segment section



dc030778938b8b6f98236a709d0d18734
Headers
.text
.rdata
.data
.reloc

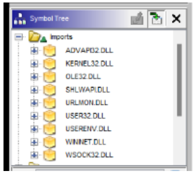
2. What are different functions, imports and exports of each Malware?

Functions



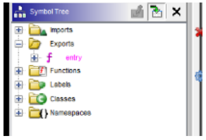
Imports
Exports
Functions
entry
FUN_1000
Labels
Classes
Namespaces

Imports



Imports
ADVAPI32.DLL
KERNEL32.DLL
OLE32.DLL
SHLWAPI.DLL
URLMON.DLL
USER32.DLL
USERENV.DLL
WININET.DLL
WSOCK32.DLL

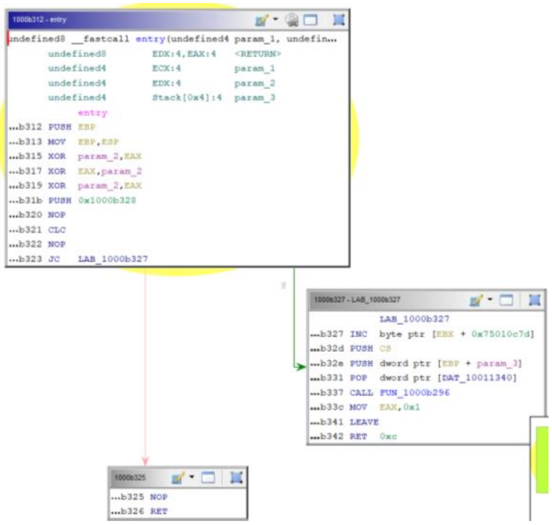
Exports



Imports
Exports
entry
Functions
Labels
Classes
Namespaces

3. What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

Function Flow

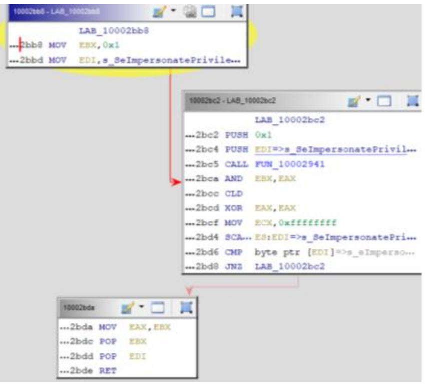


```
undefined8 __fastcall entry(undefined4 param_1, undefin...
       undefined8         EDX:4,EAX:4     <RETURN>
       undefined4         ECX:4           param_1
       undefined4         EDX:4           param_2
       undefined4         Stack[0x4]:4    param_3
            entry
...b312 PUSH EBP
...b313 MOV  EBP,ESP
...b315 XOR  param_2,EAX
...b317 XOR  EAX,param_2
...b319 XOR  param_2,EAX
...b31b PUSH 0x1000b328
...b320 NOP
...b321 CLC
...b322 NOP
...b323 JC   LAB_1000b327
```

```
            LAB_1000b327
...b327 INC  byte ptr [EBX + 0x75010c7d]
...b32d PUSH CS
...b32e PUSH dword ptr [EBP + param_3]
...b331 POP  dword ptr [DAT_10011340]
...b337 CALL FUN_1000b296
...b33c MOV  EAX,0x1
...b341 LEAVE
...b342 RET  0xc
```

```
...b325 NOP
...b326 RET
```

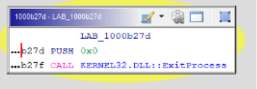
Suspicious Functions



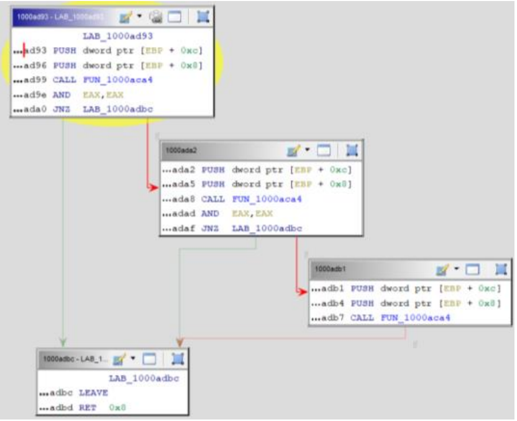
```
            LAB_10002bb8
...2bb8 MOV  EBX,0x1
...2bbd MOV  EDI,s_SeImpersonatePrivile...
```

```
            LAB_10002bc2
...2bc2 PUSH 0x1
...2bc4 PUSH EDI=>s_SeImpersonatePrivil...
...2bc5 CALL FUN_10002941
...2bca AND  EBX,EAX
...2bcc CLD
...2bcd XOR  EAX,EAX
...2bcf MOV  ECX,0xffffffff
...2bd4 SCA... ES:EDI=>s_SeImpersonatePri...
...2bd6 CMP  byte ptr [EDI]=>s_eImperso...
...2bd8 JNZ  LAB_10002bc2
```

```
...2bda MOV  EAX,EBX
...2bdc POP  EBX
...2bdd POP  EDI
...2bde RET
```



```
            LAB_1000b27d
...b27d PUSH 0x0
...b27f CALL KERNEL32.DLL::ExitProcess
```



```
            LAB_1000ad93
...ad93 PUSH dword ptr [EBP + 0xc]
...ad96 PUSH dword ptr [EBP + 0x8]
...ad99 CALL FUN_1000aca4
...ad9e AND  EAX,EAX
...ada0 JNZ  LAB_1000adbc
```

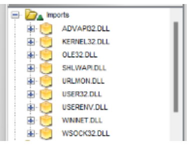
```
...ada2 PUSH dword ptr [EBP + 0xc]
...ada5 PUSH dword ptr [EBP + 0x8]
...ada8 CALL FUN_1000aca4
...adad AND  EAX,EAX
...adaf JNZ  LAB_1000adbc
```

```
...adb1 PUSH dword ptr [EBP + 0xc]
...adb4 PUSH dword ptr [EBP + 0x8]
...adb7 CALL FUN_1000aca4
```

```
            LAB_1000adbc
...adbc LEAVE
...adbd RET  0x8
```

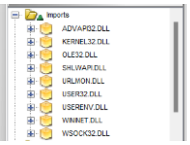
4. What DLL’s any malware includes? Is there any suspicious functionality called by these DLL’s?

DLL



```
Imports
  ADVAPI32.DLL
  KERNEL32.DLL
  OLE32.DLL
  SHLWAPI.DLL
  URLMON.DLL
  USER32.DLL
  USERENV.DLL
  WININET.DLL
  WSOCK32.DLL
```

Suspicious Dll

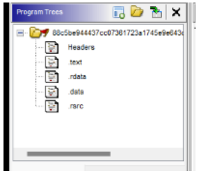


```
Imports
  ADVAPI32.DLL
  KERNEL32.DLL
  OLE32.DLL
  SHLWAPI.DLL
  URLMON.DLL
  USER32.DLL
  USERENV.DLL
  WININET.DLL
  WSOCK32.DLL
```

- in32/Tnega.bXRKZUB

1. What are the different segments or sections in case of each malware?

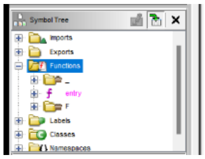
Segment section



```
88c5be944437cc07361723a1745e9e643c
  Headers
  .text
  .rdata
  .data
  .rsrc
```

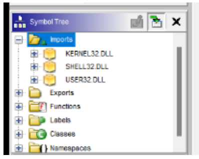
2. What are different functions, imports and exports of each Malware?

Function



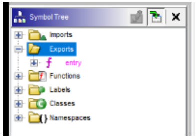
```
Imports
Exports
Functions
  _
  entry
  F
Labels
Classes
Namespaces
```

Imports



```
Imports
  KERNEL32.DLL
  SHELL32.DLL
  USER32.DLL
Exports
Functions
Labels
Classes
Namespaces
```

Exports



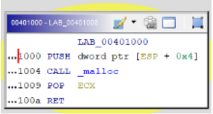
```
Imports
Exports
  entry
Functions
Labels
Classes
Namespaces
```

3. What is flow of functions in case of each malware? Is there any suspicious

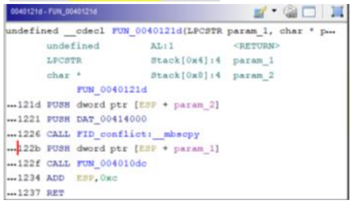
function? Give detail (name, arguments, call mechanism) of suspicious functions?

Function Flow

Suspicious Functions



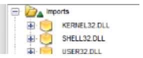
```
                LAB_00401000
...1000 PUSH  dword ptr [ESP + 0x4]
...1004 CALL  _malloc
...1009 POP   ECX
...100a RET
```



```
undefined __cdecl FUN_0040121d(LPCSTR param_1, char * p...
      undefined          AL:1          <RETURN>
      LPCSTR             Stack[0x4]:4  param_1
      char *             Stack[0x8]:4  param_2
                  FUN_0040121d
...121d PUSH  dword ptr [ESP + param_2]
...1221 PUSH  DAT_00414000
...1226 CALL  FID_conflict:__mbscpy
...122b PUSH  dword ptr [ESP + param_1]
...122f CALL  FUN_004010dc
...1234 ADD   ESP,0xc
...1237 RET
```

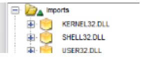
4. What DLL's any malware includes? Is there any suspicious functionality called by these DLL's?

Dll



```
Imports
    KERNEL32.DLL
    SHELL32.DLL
    USER32.DLL
```

Suspicious Dll

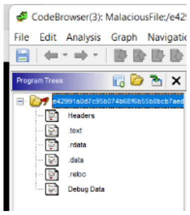


```
Imports
    KERNEL32.DLL
    SHELL32.DLL
    USER32.DLL
```

- W32.SecretKAN.Trojan

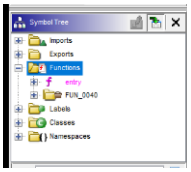
1. What are the different segments or sections in case of each malware?

Segments section

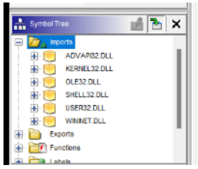

CodeBrowser(3): MalaciousFile:/e42
File Edit Analysis Graph Navigatic
Program Trees
e42991a0d7c95b074b68f6b55b8bcb7aed
Headers
.text
.rdata
.data
.reloc
Debug Data

2. What are different functions, imports and exports of each Malware?

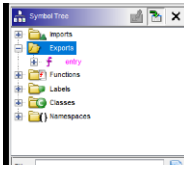
Functions



Imports

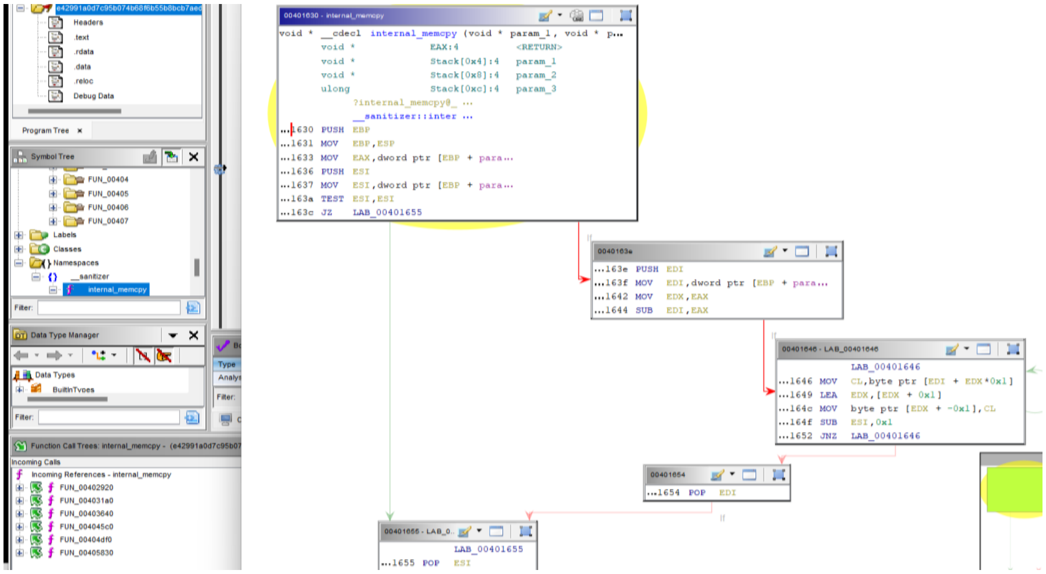


Exports



3. What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?

Flow of function



e42991a0d7c95b074b68f6b55b8bcb7aed
Headers
.text
.rdata
.data
.reloc
Debug Data

Program Tree

Symbol Tree
FUN_00404
FUN_00405
FUN_00406
FUN_00407
Labels
Classes
Namespaces
__sanitizer
internal_memcpy

Data Type Manager
Data Types
BuiltInTypes

Function Call Trees: internal_memcpy - (e42991a0d7c95b07
Incoming Calls
Incoming References - internal_memcpy
FUN_00402920
FUN_004031a0
FUN_00403640
FUN_004045c0
FUN_00404df0
FUN_00405830

```
00401630 - internal_memcpy
void * __cdecl internal_memcpy (void * param_1, void * p…
       void *            EAX:4          <RETURN>
       void *            Stack[0x4]:4   param_1
       void *            Stack[0x8]:4   param_2
       ulong             Stack[0xc]:4   param_3
             ?internal_memcpy@_ …
             __sanitizer::inter …
…1630 PUSH  EBP
…1631 MOV   EBP,ESP
…1633 MOV   EAX,dword ptr [EBP + para…
…1636 PUSH  ESI
…1637 MOV   ESI,dword ptr [EBP + para…
…163a TEST  ESI,ESI
…163c JZ    LAB_00401655
```

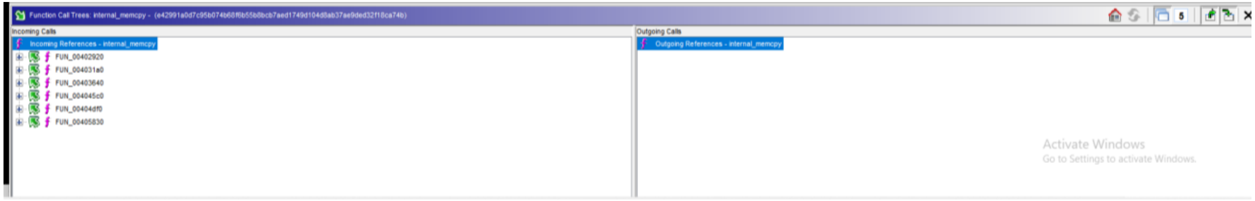
```
0040163e
…163e PUSH  EDI
…163f MOV   EDI,dword ptr [EBP + para…
…1642 MOV   EDX,EAX
…1644 SUB   EDI,EAX
```

```
00401646 - LAB_00401646
             LAB_00401646
…1646 MOV   CL,byte ptr [EDI + EDX*0x1]
…1649 LEA   EDX,[EDX + 0x1]
…164c MOV   byte ptr [EDX + -0x1],CL
…164f SUB   ESI,0x1
…1652 JNZ   LAB_00401646
```

```
00401654
…1654 POP   EDI
```

```
00401655 - LAB_0…
             LAB_00401655
…1655 POP   ESI
```

Suspicious function



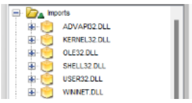
Function Call Trees: internal_memcpy - (e42991a0d7c95b074b68f6b55b8bcb7aed1749d104d8ab37ae9ded32f18ca74b)

Incoming Calls
Incoming References - internal_memcpy
FUN_00402920
FUN_004031a0
FUN_00403640
FUN_004045c0
FUN_00404df0
FUN_00405830

Outgoing Calls
Outgoing References - internal_memcpy

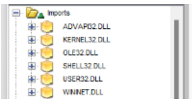
4. What DLL's any malware includes? Is there any suspicious functionality called by these DLL's?

DLL



Imports
ADVAPI32.DLL
KERNEL32.DLL
OLE32.DLL
SHELL32.DLL
USER32.DLL
WININET.DLL

Suspicious dll



Imports
ADVAPI32.DLL
KERNEL32.DLL
OLE32.DLL
SHELL32.DLL
USER32.DLL
WININET.DLL