Target Analysis Report

1. Static Analysis

(1) File Info

Field	Value
Target File Path	C:\Users\User\Desktop\DestDir\04.exe
Hashes	MD5: 70d41eadb33a9d48d112031733406655 SHA1: 013c77d3050346bcb2af4a49b141320467ed8e41 SHA256: d36727b07105a6d517cc0b0919770d027a938b7c5cb6784572cfe346a87c4815
Extension	.exe
MIME Type	application/x-dosexec
PE Signature	MZ_signature: 4D5A PE_signature: 50450000 PE_offset: 0xE8

(2) PE Analysis

1. Sections

Section Name	Size	Entropy
.text	196608	4.11
.rdata	12288	3.75
.data	20480	0.78
.idata	4096	2.64
.reloc	8192	4.91

Library: KERNEL32.dll

Suspicious Functions
IsDebuggerPresent
TerminateProcess
WriteFile
GetProcAddress
LoadLibraryA
CloseHandle
ReadFile

(3) LLM Analysis Result

Field	Value

probability	0.9707
LLM Result	Malware

2. Dynamic Analysis

(1) API Monitor

Thread ID: 1100 / Type : Anti-Debugging

Type	Count
Ransomware	0
Loader	0
Infostealer	0
RAT	0
Enumeration	0
Injection	1
Evasion	196
Spying	0
Internet	0
Anti-Debugging	294
Helper	98

Thread ID: 10932 / Type : Injection

Type	Count
Ransomware	0
Loader	0
Infostealer	0
RAT	0
Enumeration	0
Injection	2
Evasion	0
Spying	0
Internet	0
Anti-Debugging	0
Helper	1

Thread ID: 10428 / Type : Injection

Type	Count
Ransomware	0
Loader	0
Infostealer	0
RAT	0

Enumeration	0
Injection	2
Evasion	0
Spying	0
Internet	0
Anti-Debugging	0
Helper	1

Thread ID: 11196 / Type : Injection

Type	Count
Ransomware	0
Loader	0
Infostealer	0
RAT	0
Enumeration	0
Injection	2
Evasion	0
Spying	0
Internet	0
Anti-Debugging	0
Helper	1

(2) Event Monitor

Event ID: 4672

Field	Value
event_provider	Microsoft-Windows-Security-Auditing
event_message	S-1-5-18 | SYSTEM | NT AUTHORITY | 0x3e7 | SeAssignPrimaryTo...
count	3526

Event ID: 4624

Field	Value
event_provider	Microsoft-Windows-Security-Auditing
event_message	S-1-5-18 | WINDEV2407EVAL$ | WORKGROUP | 0x3e7 | S-1-5-18 | ...
count	3765

Event ID: 4625

Field	Value
event_provider	Microsoft-Windows-Security-Auditing
event_message	S-1-5-18 | WINDEV2407EVAL$ | WORKGROUP | 0x3e7 | S-1-0-0 | U...
count	71

Event ID: system

Field	Value
event_provider	N/A
event_message	N/A
count	N/A

(3) Network Monitor

IP Port List
10.0.2[.]15:49818
10.0.2[.]15:5353
10.0.2[.]15:55649
10.0.2[.]15:57285
10.0.2[.]15:57443
13.107.246[.]74:443
168.126.63[.]1:53
224.0.0[.]251:5353

(4) Memory Monitor

Process List

Process List
Runtime.exe
g.exe
lsass.exe
notepad.exe
cmd.exe
gspawn-win32-helper-console.exe
04.exe
prototype.exe
gspawn-win32-helper.exe
v8.exe

Strings

Strings
MDMP
AuthenticAMD
9+1'
z:y`F#
]#S{X$
});
}
});
NB10
Z:_My Project\CodeEngn\Challenge v2.0\Reverse\04\src\Debug\01-IsDebuggerPresent.pdb

(5) Registry Monitor

Modified

Registry
Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx

(6) Final Type

Field	Value
Type	Anti-Debugging

Appendix

Library: KERNEL32.dll

Suspicious Functions	Entire Functions
IsDebuggerPresent	IsDebuggerPresent
TerminateProcess	Sleep
WriteFile	MultiByteToWideChar
GetProcAddress	GetCommandLineA
LoadLibraryA	GetVersion
CloseHandle	ExitProcess
ReadFile	RtlUnwind
	RaiseException
	IsBadWritePtr
	IsBadReadPtr
	HeapValidate
	TerminateProcess
	GetCurrentProcess
	DebugBreak
	GetStdHandle
	WriteFile
	InterlockedDecrement
	OutputDebugStringA
	GetProcAddress
	LoadLibraryA
	InterlockedIncrement
	GetModuleFileNameA
	UnhandledExceptionFilter
	FreeEnvironmentStringsA
	FreeEnvironmentStringsW
	WideCharToMultiByte
	GetEnvironmentStrings
	GetEnvironmentStringsW
	SetHandleCount
	GetFileType
	GetStartupInfoA
	GetModuleHandleA
	GetEnvironmentVariableA
	GetVersionExA
	HeapDestroy
	HeapCreate
	HeapFree
	VirtualFree
	GetLastError

	SetFilePointer
	FlushFileBuffers
	CloseHandle
	SetUnhandledExceptionFilter
	HeapAlloc
	HeapReAlloc
	VirtualAlloc
	SetConsoleCtrlHandler
	GetCPInfo
	GetACP
	GetOEMCP
	IsBadCodePtr
	ReadFile
	SetStdHandle
	GetStringTypeA
	GetStringTypeW
	LCMapStringA
	LCMapStringW

API/Function Calls

Thread ID: 1100

API/Function
IsDebuggerPresent
RtlDelayExecution
RtlRunOnceBeginInitialize
LdrpResGetMappingSize
RtlReAllocateHeap
ZwDelayExecution
RtlNumberOfSetBitsUlongPtr
GetNumaNodeProcessorMask2
SleepEx
RtlGetCurrentServiceSessionId
WriteFile
ZwWriteFile
NtAllocateVirtualMemory
RtlInitializeCriticalSectionEx
RtlAllocateHeap
RtlInterlockedCompareExchange64
RtlWow64GetEquivalentMachineCHPE
Sleep

Thread ID: 10932

API/Function
RtlDebugPrintTimes
TpCallbackIndependent
RtlDisownModuleHeapAllocation
RtlLeaveCriticalSection
RtlFreeActivationContextStack
TpWorkOnBehalfSetTicket
NtQueryInformationThread
RtlAcquireSRWLockShared
RtlFreeHeap
RtlAcquireSRWLockExclusive
RtlExitUserThread
MicrosoftTelemetryAssertTriggeredUM
RtlNumberOfSetBitsUlongPtr

LdrShutdownThread
TpWorkOnBehalfClearTicket
RtlFreeThreadActivationContextStack
memcmp
ZwTerminateThread
RtlGetGroupSecurityDescriptor
RtlGetCurrentServiceSessionId
RtlRemovePropertyStore
TpCheckTerminateWorker
RtlReleaseSRWLockShared
RtlReleaseSRWLockExclusive
RtlInterlockedCompareExchange64
RtlGetImageFileMachines

Thread ID: 10428

API/Function
RtlFormatMessageEx
RtlDebugPrintTimes
TpCallbackIndependent
RtlDisownModuleHeapAllocation
RtlClearThreadWorkOnBehalfTicket
RtlLeaveCriticalSection
RtlFreeActivationContextStack
TpWorkOnBehalfSetTicket
NtQueryInformationThread
RtlAcquireSRWLockShared
RtlFreeHeap
RtlAcquireSRWLockExclusive
memset
NtWaitForWorkViaWorkerFactory
RtlExitUserThread
RtlNumberOfSetBitsUlongPtr
RtlSetThreadWorkOnBehalfTicket
LdrShutdownThread
TpWorkOnBehalfClearTicket
RtlFreeThreadActivationContextStack
memcmp
ZwTerminateThread

RtlGetGroupSecurityDescriptor
RtlRetrieveNtUserPfn
RtlGetCurrentServiceSessionId
RtlUTF8ToUnicodeN
RtlGetImageFileMachines
RtlRemovePropertyStore
TpCheckTerminateWorker
EtwpGetCpuSpeed
RtlReleaseSRWLockShared
RtlReleaseSRWLockExclusive
RtlEnterCriticalSection
RtlInterlockedCompareExchange64
MicrosoftTelemetryAssertTriggeredUM

Thread ID: 11196

API/Function
RtlDebugPrintTimes
TpCallbackIndependent
RtlDisownModuleHeapAllocation
RtlLeaveCriticalSection
RtlFreeActivationContextStack
TpWorkOnBehalfSetTicket
NtQueryInformationThread
RtlAcquireSRWLockShared
RtlFreeHeap
RtlAcquireSRWLockExclusive
RtlExitUserThread
MicrosoftTelemetryAssertTriggeredUM
RtlNumberOfSetBitsUlongPtr
LdrShutdownThread
TpWorkOnBehalfClearTicket
RtlFreeThreadActivationContextStack
memcmp
ZwTerminateThread
RtlGetGroupSecurityDescriptor
RtlGetCurrentServiceSessionId
RtlRemovePropertyStore
TpCheckTerminateWorker

RtlReleaseSRWLockShared
RtlReleaseSRWLockExclusive
RtlInterlockedCompareExchange64
RtlGetImageFileMachines

Network Traffic

Protocol	Src:Port	Dst:Port	Payload Len
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:57443	168.126.63[.]1:53	
UDP	10.0.2[.]15:57285	168.126.63[.]1:53	
UDP	168.126.63[.]1:53	10.0.2[.]15:57285	
UDP	168.126.63[.]1:53	10.0.2[.]15:57443	
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	1793
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	99
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	607
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1176
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1441
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	74
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	92
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	272
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	667
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	31
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460

TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1088
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1274
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	904
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1398
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1150
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	778
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460

TCP	13.107.246[.]74:443	10.0.2[.]15:49818	1460
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	481
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	
UDP	10.0.2[.]15:55649	168.126.63[.]1:53	
UDP	168.126.63[.]1:53	10.0.2[.]15:55649	
TCP	10.0.2[.]15:49818	13.107.246[.]74:443	1
TCP	13.107.246[.]74:443	10.0.2[.]15:49818	
UDP	10.0.2[.]15:5353	224.0.0[.]251:5353	