

2 - 4 October, 2024 / Dublin, Ireland

# AUTOMATICALLY DETECT AND SUPPORT AGAINST ANTI-DEBUG WITH IDA/GHIDRA TO STREAMLINE DEBUGGING PROCESS

Takahiro Takeda

LAC Cyber Emergency Center, Japan

takahiro.takeda@lac.co.jp

www.virusbulletin.com

## ABSTRACT

Malware authors often employ anti-debugging techniques to obstruct analysis. When executed on a debugger, the malware detects the debugger and either stops its subsequent actions or behaves differently from usual, making analysis difficult. The number of anti-debugging implementations varies with each malware. Notably, malware spread through mass-mailing campaigns that affect many organizations, and popular ransomware, have been confirmed to possess multiple anti-debugging techniques. For example, anti-debugging techniques include VM detection, which checks for a debugging environment, detection of breakpoints (which temporarily pause program execution during debugging), and time difference detection, which utilizes the difference in execution time when analysing malware with a debugger.

'AntiDebugSeeker' is an open-source plugin for the binary analysis tools IDA and Ghidra, which are frequently utilized by analysts. It streamlines the malware analysis process by automatically identifying the anti-debugging techniques embedded within *Windows* malware. Code with anti-debug capabilities often overlaps with techniques used for anti-analysis, as well as with the preparatory steps for process injection, which are frequently employed by malware. Therefore, by flexibly customizing the detection rules, it is possible not only to identify anti-debugging features but also to understand the functionalities of the malware. Furthermore, the tool also provides functionalities to explain these anti-debugging measures and approaches to the corresponding functions. This enhances the analyst's ability to understand and counteract the malware's evasion techniques effectively, offering a more comprehensive understanding and response strategy against such threats. This paper provides a comprehensive explanation of AntiDebugSeeker, detailing its features and usage. It offers an in-depth understanding of the tool and illustrates how these features can effectively be applied in various threat scenarios.

## INTRODUCTION OF ANTIDEBUGSEEKER

AntiDebugSeeker is a program for automatically identifying and extracting potential anti-debugging techniques used by malware and displaying them in IDA [1] or Ghidra [2].

The main functionalities of this plugin are as follows:

- 1. Extraction of APIs that are potentially being used by the malware for anti-debugging.
- 2. In addition to APIs, extraction of anti-debugging techniques based on key phrases that serve as triggers, as some anti-debugging methods cannot be comprehensively identified by API calls alone.

As a note, for packed samples, it is more effective to run this plugin after unpacking and fixing the Import Address Table.

# ANTIDEBUGSEEKER FOR IDA

#### Files required to run the program

For the purpose of facilitating the detection of anti-debugging techniques using IDA, the following three files must be placed within the plugin directory of the IDA software:

- anti\_debug.config this file contains a set of rules designed to identify various anti-debugging techniques.
- anti\_debug\_techniques\_descriptions.json this file provides detailed descriptions of the rules detected.
- AntiDebugSeeker.py this script serves as the core program for anti-debugging detection.

C:	C:¥Program Files¥IDA Pro 8.3¥plugins				
r	<b>^</b> 名前 <sup>^</sup>	更新日時	種類	サイズ	
P	bochs	2023/09/07 9:29	ファイル フォルダー		
۴	hexrays_sdk	2023/09/07 9:29	ファイル フォルダー		
r	iconengines	2023/09/07 9:29	ファイル フォルダー		
r	imageformats	2023/09/07 9:29	ファイル フォルダー		
r	platforms	2023/09/07 9:29	ファイル フォルダー		
	printsupport	2023/09/07 9:29	ファイル フォルダー		
	sqldrivers	2023/09/07 9:29	ファイル フォルダー		
	styles	2023/09/07 9:29	ファイル フォルダー		
	🖺 anti_debug.config	2023/09/07 9:22	CONFIG ファイル	5 KB	
	anti_debug_techniques_descriptions.json	2023/08/29 13:46	JSON ファイル	9 KB	
	🕞 AntiDebugSeeker.py	2023/09/06 14:48	Python File	19 KB	
	🚳 arm_mac_stub64.dll	2023/06/09 0:50	アプリケーション拡張	177 KB	
	🚳 armlinux_stub.dll	2023/06/09 0:50	アプリケーション拡張	129 KB	
	armlinux_stub64.dll	2023/06/09 0:50	アプリケーション拡張	130 KB	

Figure 1: Three files to run in IDA.

### Regarding anti\_debug.config

The anti\_debug.config file contains rules for detecting anti-debugging features. It is divided into two sections: Anti\_Debug\_API and Anti\_Debug\_Technique.

In the Anti\_Debug\_API section, you can freely create categories and add any number of APIs you want to detect (exact match).

###Anti_Debug_API###	###Anti_Debug_API###
[Category Name]	[Debugger check]
ΔΡΙ1	CheckRemoteDebuggerPresent
	DebugActiveProcess
APIZ	DebugBreak
API3	DbgSetDebugFilterState
	DbgUiDebugActiveProcess
•	IsDebuggerPresent

Figure 2: Anti\_Debug\_API section.

In the Anti\_Debug\_Technique section, you can set up to three keywords (partial match) under a single rule name.

###Anti_Debug_Technique### default_search_range=80	<pre>###Anti_Debug_Technique### default_search_range=80</pre>
[Rule1] ABC <b>80bytes</b> DEF <b>80bytes</b> GHI <b>80bytes</b>	[NtGlobalFlag_check] fs:30h 68h 70h

Figure 3: Anti\_Debug\_Technique section.

The basic flow of the search is as follows:

The search begins with the first keyword. If it is found, the second keyword is then searched for within a specified number of bytes (the default is 80 bytes). This same process is applied when searching for the third keyword.

Search Target:

Disassembly (Opcode, Operand)

Comments

API based on Import Table

Should you wish to alter the predefined default values and tailor the search parameters, append 'search\_range=value' to the specified keyword. This adjustment facilitates the customization of the search scope for each established rule within your configuration.

###Anti_Debug_Technique### default_search_range=80
[Rule1] ABC DEF GHI search_range=50
[Rule2] JKL MNO search_range=200

Figure 4: How to specify the search range.

# Regarding anti\_debug\_techniques\_descriptions.json

This JSON file provides explanations for the rules defined in the Anti\_Debug\_Technique section of the anti\_debug.config file, detailing why they were detected and describing the rules themselves. This information can also be useful for reference in case of false detections. Comments are recorded in IDA for the addresses that were detected.



Figure 5: The contents of anti\_debug\_techniques\_descriptions.json.

### The functionality of AntiDebugSeeker

Upon activation of the plugin using the keyboard shortcut Ctrl + Shift + D, the system initiates an analysis sequence. Subsequent to the completion of this analysis, a user interface screen entitled 'Anti Debug Detection Results' will be displayed. This interface presents the findings of the analysis, enabling detailed examination of the detected anti-debugging techniques.

Analysis Environment Check SetupDiGetClassDevsA 0.401042 Analysis Environment Check SetupDiGetDeviceRegistryPr- 0.401068 Analysis Environment Check SetupDiGetDeviceRegistryPr- 0.401068 Analysis Environment Check SetupDiGetDeviceRegistryPr- 0.401068 Analysis Environment Check SetupDiGetDeviceRegistryPr- 0.401068 Check Invalid Close->Exception CloseHandle 0.401119 Check Invalid Close->Exception CloseHandle 0.401170 Check Invalid Close->Exception CloseHandle 0.401170 Check Invalid Close->Exception CloseHandle 0.40118 Check Invalid Close->Exception CloseHandle 0.401194 Check Invalid Close->Exception CloseHandle 0.401194 Check Invalid Close->Exception CloseHandle 0.401194 Check Invalid Close->Exception CloseHandle 0.401940 Time Check Sleep 0.401940 Memory Manipulation VirtualProtectEx 0.401907 Memory Manipulation VirtualProtectEx 0.4019DD Memory Manipulation VirtualProtectEx 0.4019DD Memory Manipulation VirtualProtectEx 0.4019DD Time Check WaitForSingleObject 0.40217E Thread Kexcute ResumeThread 0.402170 Time Check WaitForSingleObject 0.402203 Time Check WaitForSingleObject 0.402203 Time Check WaitForSingleObject 0.402203 Time Check WaitForSingleObject 0.402203 Time Check WaitForSingleObject 0.402203 Check Invalid Close->Exception CloseHandle 0.402264 Thread Execute ResumeThread 0.402220 Check Invalid Close->Exception CloseHandle 0.402269 Check Invalid Close->Exception CloseHandle 0.402260 Check Invalid Close->Excep	Category Name	Possible Anti-Debug API	Address	Possible Anti-Debug Technique	Address
Analysis Environment Check SetupDiEnumDeviceInfo 0:401043 Analysis Environment Check SetupDiGetDeviceRegistryPrrv 0:401062 Analysis Environment Check SetupDiGetDeviceRegistryPrrv 0:401063 Analysis Environment Check SetupDiGetDeviceRegistryPrrv 0:401092 Check Invalid Close>-Exception CloseHandle 0:401419 Check Invalid Close>-Exception CloseHandle 0:401419 Check Invalid Close>-Exception CloseHandle 0:401419 Check Invalid Close>-Exception CloseHandle 0:401418 User Interaction Check GetCursorInfo 0:401084 Check Invalid Close>-Exception CloseHandle 0:401418 Check Invalid Close>-Exception CloseHandle 0:40170 Time Check Sleep 0:40184F Check Invalid Close>-Exception CloseHandle 0:40194D Time Check Sleep 0:40194D Time Check Sleep 0:40194D Memory Manipulation VirtualProtectEx 0:401907 Memory Manipulation VirtualProtectEx 0:40197 Memory Manipulation VirtualProtectEx 0:401917 Time Check WaitForSing80bject 0:402176 Thread Beacute ResumeThread 0:4022176 Thread Manipulation SuspenThread 0:4022C3 Time Check WaitForSing80bject 0:4022C3 Time Check GetTickCount 0:4022E4 Thread Beacute ResumeThread 0:4022C3 Time Check GetTickCount 0:4022E5 Check Invalid Close>-Exception CloseHandle 0:4022E76 Check Invalid Close>-Exception CloseHandle 0:4022E76 Check Invalid Close>-Exception CloseHandle 0:4022F66 Time Check GetTickCount 0:402F66 Time Check GetTickCount 0:402F66 Time Check GetTickCount 0:402F66 Check Invalid Close>-Exception CloseHandle 0:4022F66 Time Check GetTickCount 0:402F66 Time Check GetTickCount 0	Analysis Environment Check	SetupDiGetClassDevsA	0×401022		
Analysis Environment Check SetupDiGetDeviceRegistryPr··· 0x401062 Analysis Environment Check SetupDiGetDeviceRegistryPr··· 0x401092 Check Invalid Close>>Exception CloseHandle 0x401410 Check Invalid Close>>Exception CloseHandle 0x4014119 Check Invalid Close>>Exception CloseHandle 0x4014119 Check Invalid Close>>Exception CloseHandle 0x4014119 Check Invalid Close>>Exception CloseHandle 0x4014119 Check Invalid Close>>Exception CloseHandle 0x401414 User Interaction Check GetCursorInfo 0x40161B Check Invalid Close>>Exception CloseHandle 0x401414 Check Invalid Close>>Exception CloseHandle 0x401414 Check Invalid Close>>Exception CloseHandle 0x40184F Check Invalid Close>>Exception CloseHandle 0x40194D Time Check Sleep 0x40194A Memory Manipulation VirtualProtectEx 0x401907 Memory Manipulation VirtualProtectEx 0x401907 Memory Manipulation VirtualProtectEx 0x40191D Memory Manipulation VirtualProtectEx 0x40111 Check Invalid Close>>Exception CloseHandle 0x402170 Time Check WaitForSingBobject 0x402201 Thread Execute ResumeThread 0x402217 Thread Execute ResumeThread 0x402203 Time Check WaitForSingBobject 0x402203 Thread Execute ResumeThread 0x402203 Thread Execute ResumeThread 0x402203 Thread Execute ResumeThread 0x402203 Thread Execute ResumeThread 0x402203 Check Invalid Close>Exception CloseHandle 0x402217 Thread Execute ResumeThread 0x402203 Check Invalid Close>Exception CloseHandle 0x402217 Thread Execute ResumeThread 0x402203 Check Invalid Close>Exception CloseHandle 0x402217 Check Invalid Close>Exception CloseHandle 0x402217 Thread Execute ResumeThread 0x402203 Check Invalid Close>Exception CloseHandle 0x402217 Check Invalid Close>Exception CloseHandle 0x40225 Check Invalid Close>Exception CloseHandle 0x402263 Check Invalid Close>Exception CloseHandle 0x402263 Check Invalid Close>Exception CloseHandle 0x402266 Check Invalid Close>Exception CloseHandle 0x40227 Check Invalid Close>Exception CloseHandle 0x40227 Check Invalid Close>Exception CloseHandle 0x40227 Check Invalid Close>E	Analysis Environment Check	SetupDiEnumDeviceInfo	0×401043		
Analysis Environment Check SetupDiGetDeviceRegistryPr-·· 0x401088 Analysis Environment Check SetupDiGetDeviceRegistryPr-·· 0x401092 Check Invalid Close→Exception CloseHandle 0x401419 Check Invalid Close→Exception CloseHandle 0x401419 User Interaction Check GetCursorInfo 0x40161B Check Invalid Close→Exception CloseHandle 0x401707 Time Check Seep 0x40184F Check Invalid Close→Exception CloseHandle 0x40184F Check Invalid Close→Exception CloseHandle 0x40185D Check Invalid Close→Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Time Check Sleep 0x40194D Time Check Sleep 0x40194D Memory Manipulation VirtualProtectEx 0x40190C Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation SuspendThread 0x402170 Time Check WaitForSingleObject 0x402171 Time Check WaitForSingleObject 0x402201 Thread Execute ResumeThread 0x402203 Check Invalid Close→Exception CloseHandle 0x402265 Check Invalid Close→Exception CloseHandle 0x402260 Check Invalid Close→Exception CloseHandle 0x40266 Ti	Analysis Environment Check	SetupDiGetDeviceRegistryPr…	0×401062		
Analysis Environment Check SetupDiGetDeviceRegistryPr~ 0x401092 Check Invalid Close→Exception CloseHandle 0x401419 Check Invalid Close→Exception CloseHandle 0x401419 Check Invalid Close→Exception CloseHandle 0x40161E User Interaction Check GetCursorInfo 0x40161E Check Invalid Close→Exception CloseHandle 0x401707 Time Check Sleep 0x40184F Check Invalid Close→Exception CloseHandle 0x40185D Check Invalid Close→Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Time Check WaitForSingleObject 0x4019D Time Check WaitForSingleObject 0x402170 Thread Manipulation SuspendThread 0x402170 Thread Manipulation SuspendThread 0x402203 Thread Manipulation SuspendThread 0x402201 Thread Manipulation SuspendThread 0x402201 Thread Manipulation SuspendThread 0x402220 Thread Manipulation SuspendThread 0x402220 Check Invalid Close→Exception CloseHandle 0x40225B Check Invalid Close→Exception CloseHandle 0x402264 Thread Execute ResumeThread 0x402220 Check Invalid Close→Exception CloseHandle 0x402265 Check Invalid Close→Exception CloseHandle 0x402266 Check Invalid Close→Exception CloseHandle 0x402266 Time Check GetTickCount 0x402266 Check Invalid Close→Exception CloseHandle 0x4022	Analysis Environment Check	SetupDiGetDeviceRegistryPr…	0×401068		
Check Invalid Close->Exception CloseHandle 0x401410 Check Invalid Close->Exception CloseHandle 0x401419 Check Invalid Close->Exception CloseHandle 0x40161B Check Invalid Close->Exception CloseHandle 0x401707 Time Check Invalid Close->Exception CloseHandle 0x401707 Time Check Invalid Close->Exception CloseHandle 0x40184F Check Invalid Close->Exception CloseHandle 0x40185D Check Invalid Close->Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Memory Manipulation VirtualProtectEx 0x40190D Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x40117 Time Check Resume Thread 0x402170 Thread Execute Resume Thread 0x402170 Thread Execute Resume Thread 0x402191 Thread Execute Resume Thread 0x402203 Time Check WaitForSingleObject 0x402191 Thread Manipulation SuspendThread 0x402201 Thread Manipulation SuspendThread 0x402201 Thread Manipulation SuspendThread 0x402243 Check Invalid Close->Exception CloseHandle 0x4025B Check Invalid Close->Exceptio	Analysis Environment Check	SetupDiGetDeviceRegistryPr…	0×401092		
Check Invalid Close->Exception CloseHandle 0x401419 Check Invalid Close->Exception CloseHandle 0x40111E User Interaction Check GetCursorInfo 0x401101B Check Invalid Close->Exception CloseHandle 0x401707 Time Check Sleep 0x40185D Check Invalid Close->Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Time Check Sleep 0x40194D Time Check Sleep 0x40194D Memory Manipulation VirtualProtectEx 0x401907 Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x4019D Time Check WaitForSingleObject 0x40217E Thread Execute ResumeThread 0x40217E Thread Manipulation SuspendThread 0x4022D1 Thread Kecute ResumeThread 0x4022D1 Thread Execute ResumeThread 0x4022E4 Thread Manipulation SuspendThread 0x4022E4 Thread Manipulation Close+Tandle 0x4022E4 Check Invalid Close->Exception CloseHandle 0x4022B3 Check Invalid Close->Exception CloseHandle 0x4022D1 Thread Kecute ResumeThread 0x4022E6 Check Invalid Close->Exception CloseHandle 0x4022D1 Thread Manipulation SuspendThread 0x4022E6 Check Invalid Close->Exception CloseHandle 0x402E60 Check Invalid Close->Exception CloseHandle 0x402E760 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Check Invalid Close->Exception CloseHandle 0x40256 Check Invalid Close->Exception CloseHandle 0x402F6 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x402E76 Time Check GetTickCount 0x4	Check Invalid Close->Exception	CloseHandle	0×401410		
Check Invalid Close->Exception CloseHandle 0x40141E User Interaction Check GetOursorInfo 0x40161B Check Invalid Close->Exception CloseHandle 0x401707 Time Check Sleep 0x40184F Check Invalid Close->Exception CloseHandle 0x40194D Check Invalid Close->Exception CloseHandle 0x40194D Time Check Sleep 0x4019AB Memory Manipulation VirtualProtectEx 0x4019C7 Memory Manipulation VirtualProtectEx 0x4019D Memory Manipulation VirtualProtectEx 0x4019D Thread Execute ResumeThread 0x402170 Time Check WaitForSingleObject 0x402170 Thread Execute ResumeThread 0x402203 Time Check WaitForSingleObject 0x402203 Time Check ResumeThread 0x402203 Time Check ResumeThread 0x402203 Time Check ResumeThread 0x402203 Time Check Invalid Close->Exception CloseHandle 0x402203 Time Check ResumeThread 0x402203 Thread Execute ResumeThread 0x402235B Check Invalid Close->Exception CloseHandle 0x402423 Check Invalid Close->Exception CloseHandle 0x402265 Check Invalid Close->Exception CloseHandle 0x402266 Check Invalid Close->Exception CloseHandle 0x40266 Check Invalid	Check Invalid Close->Exception	CloseHandle	0×401419		
User Interaction Check       GetCursorInfo       0x40161E         Check Invalid Close->Exception       CloseHandle       0x401707         Time Check       Sleep       0x40184E         Check Invalid Close->Exception       CloseHandle       0x40198D         Check Invalid Close->Exception       CloseHandle       0x40194D         Check Invalid Close->Exception       CloseHandle       0x40194D         Wemory Manipulation       VirtualProtectEx       0x401907         Memory Manipulation       VirtualProtectEx       0x40185D         Memory Manipulation       VirtualProtectEx       0x401907         Memory Manipulation       VirtualProtectEx       0x40185D         Time Check       WaitForSingleObject       0x401835         Thread Execute       ResumeThread       0x401835         Thread Execute       ResumeThread       0x401217E         Thread Banipulation       SuspendThread       0x402203         Time Check       WaitForSingleObject       0x402263         Time Check       WaitForSingleObject       0x402242         Check Invalid Close->Exception       CloseHandle       0x402256         Check Invalid Close->Exception       CloseHandle       0x402260         Check Invalid Close->Exception       CloseHandle	Check Invalid Close->Exception	CloseHandle	0×40141E		
Opened_Exclusively_Check       0x4016cf         Check Invalid Close->Exception CloseHandle       0x401707         Time Check       Sleep       0x40185D         Check Invalid Close->Exception CloseHandle       0x40194D         Time Check       Sleep       0x40194D         Time Check       Sleep       0x40194D         Memory Manipulation       VirtualProtectEx       0x401907         Memory Manipulation       VirtualProtectEx       0x401910D         Memory Manipulation       VirtualProtectEx       0x401185         Check Invalid Close->Exception CloseHandle       0x401907         Memory Manipulation       VirtualProtectEx       0x401910D         Memory Manipulation       VirtualProtectEx       0x401170         Memory Manipulation       VirtualProtectEx       0x401170         Memory Manipulation       VirtualProtectEx       0x402170         Time Check       ResumeThread       0x402170         Time Check       WaitForSingleObject       0x402203         Time Check       WaitForSingleObject       0x402203         Time Check       ResumeThread       0x4022040         Check Invalid Close->Exception CloseHandle       0x4022040         Check Invalid Close->Exception CloseHandle       0x402403	User Interaction Check	GetCursorInfo	0×40161B		
Check Invalid Close->Exception CloseHandle 0x401707 Time Check Sleep 0x40184F Check Invalid Close->Exception CloseHandle 0x40185D Check Invalid Close->Exception CloseHandle 0x40194D Time Check Sleep 0x4019A8 Memory Manipulation VirtualProtectEx 0x401907 Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x4019DD Time Check Invalid Close->Exception CloseHandle 0x401235 Thread Execute ResumeThread 0x402170 Time Check WaitForSingleObject 0x402217E Thread Manipulation SuspendThread 0x402191 Thread Execute ResumeThread 0x402217 Thread Manipulation SuspendThread 0x402217 Thread Execute ResumeThread 0x402201 Thread Manipulation SuspendThread 0x402203 Time Check WaitForSingleObject 0x402204 Check Invalid Close->Exception CloseHandle 0x402285 Check Invalid Close->Exception CloseHandle 0x402285 Check Invalid Close->Exception CloseHandle 0x402285 Check Invalid Close->Exception CloseHandle 0x402285 Check Invalid Close->Exception CloseHandle 0x402403 Check Invalid Close->Exception CloseHandle 0x402265 Time Check GetTickCount 0x402260 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close->Exception CloseHandle 0x402F66 Check Invalid Close->Exception Close				Opened_Exclusively_Check	0×4016cf
Time Check       Sleep       0x40184F         Check Invalid Close->Exception       CloseHandle       0x40194D         Time Check       Sleep       0x40194D         Time Check       Sleep       0x40194B         Memory Manipulation       VirtualProtectEx       0x40190D         Memory Manipulation       VirtualProtectEx       0x4019DD         Memory Manipulation       VirtualProtectEx       0x401855         Check Invalid Close->Exception       CloseHandle       0x401235         Thread Execute       ResumeThread       0x402170         Time Check       WaitForSingleObject       0x4022C3         Time Check       WaitForSingleObject       0x4022251         Thread Execute       ResumeThread       0x402258         Check Invalid Close->Exception       CloseHandle       0x4022409         Check Invalid Close->Exception       CloseHandle       0x402258         Check Invalid Close->Exception       CloseHandle       0x4022409         Check Invalid Close->Exception       CloseHandle       0x402259         Check Invalid Close->Exception       CloseHandle       0x4022409         Check Invalid Close->Exception       CloseHandle       0x402250         Check Invalid Close->Exception       CloseHandle	Check Invalid Close->Exception	CloseHandle	0×401707		
Check Invalid Close→Exception CloseHandle 0x40185D Check Invalid Close→Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Memory Manipulation VirtualProtectEx 0x401907 Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x40111 Check Invalid Close→Exception CloseHandle 0x401175 Time Check WaitForSingleObject 0x402170 Time Check WaitForSingleObject 0x402191 Thread Execute ResumeThread 0x402191 Thread Execute ResumeThread 0x402203 Time Check WaitForSingleObject 0x402201 Thread Manipulation SuspendThread 0x402203 Thread Execute ResumeThread 0x402264 Thread Execute ResumeThread 0x402264 Check Invalid Close→Exception CloseHandle 0x402499 Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402E60 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x4022F4	Time Check	Sleep	0×40184F		
Check Invalid Close→Exception CloseHandle 0x40194D Time Check Sleep 0x40194D Memory Manipulation VirtualProtectEx 0x4019C7 Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x4019DD Memory Manipulation VirtualProtectEx 0x4011C Check Invalid Close→Exception CloseHandle 0x401125 Thread Execute ResumeThread 0x402170 Time Check WaitForSingleObject 0x40217E Thread Manipulation SuspendThread 0x402171 Thread Execute ResumeThread 0x402171 Thread Execute ResumeThread 0x402172 Thread Execute ResumeThread 0x402203 Time Check WaitForSingleObject 0x4022D1 Thread Execute ResumeThread 0x4022E4 Thread Execute ResumeThread 0x40225B Check Invalid Close→Exception CloseHandle 0x40243 Check Invalid Close→Exception CloseHandle 0x40225D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402F60 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x4022F6	Check Invalid Close->Exception	CloseHandle	0×40185D		
Time Check       Sleep       0x4019A8         Memory Manipulation       VirtualProtectEx       0x401907         Memory Manipulation       VirtualProtectEx       0x4019DD         Memory Manipulation       VirtualProtectEx       0x4019DD         Memory Manipulation       VirtualProtectEx       0x40119DD         Memory Manipulation       VirtualProtectEx       0x4011411         Check Invalid Close->Exception       CloseHandle       0x402170         Time Check       WaitForSingleObject       0x40217E         Thread Execute       ResumeThread       0x402203         Time Check       WaitForSingleObject       0x402203         Time Check       WaitForSingleObject       0x402203         Time Check       WaitForSingleObject       0x402203         Time Check       WaitForSingleObject       0x402254         Thread Execute       ResumeThread       0x402254         Thread Execute       ResumeThread       0x4022409         Check Invalid Close->Exception       CloseHandle       0x402243         Check Invalid Close->Exception       CloseHandle       0x402250         Check Invalid Close->Exception       CloseHandle       0x402250         Check Invalid Close->Exception       CloseHandle       0x402260 <td>Check Invalid Close-&gt;Exception</td> <td>CloseHandle</td> <td>0×40194D</td> <td></td> <td></td>	Check Invalid Close->Exception	CloseHandle	0×40194D		
Memory Manipulation     VirtualProtectEx     0x401907       Memory Manipulation     VirtualProtectEx     0x4019DD       Memory Manipulation     VirtualProtectEx     0x4019DD       Memory Manipulation     VirtualProtectEx     0x40119DD       Memory Manipulation     VirtualProtectEx     0x40119D       Memory Manipulation     VirtualProtectEx     0x40117       Check Invalid Close→Exception     CloseHandle     0x402170       Time Check     WaitForSingleObject     0x402191       Thread Execute     ResumeThread     0x402203       Time Check     WaitForSingleObject     0x402203       Thread Execute     ResumeThread     0x402203       Check Invalid Close→Exception     CloseHandle     0x402258       Check Invalid Close→Exception     CloseHandle     0x402409       Check Invalid Close→Exception     CloseHandle     0x402258       Check Invalid Close→Exception     CloseHandle     0x402258       Check Invalid Close→Exception     CloseHandle     0x402258       Check Invalid Close→Exception     CloseHandle     0x402266       Check Invalid Close→Exception     CloseHandle     0x402250       Time Check     GetTickCount     0x402560       Time Check     GetTickCount     0x40266       Time Check     GetTickCount	Time Check	Sleep	0×4019A8		
Memory Manipulation       VirtualProtectEx       0x4019DD         Memory Manipulation       VirtualProtectEx       0x4019DD         Memory Manipulation       VirtualProtectEx       0x401111         Check Invalid Close→Exception       CloseHandle       0x4012170         Time Abex       WaitForSingleObject       0x402170         Time Check       WaitForSingleObject       0x402191         Thread Manipulation       SuspendThread       0x402203         Time Check       WaitForSingleObject       0x402201         Thread Manipulation       SuspendThread       0x4022E4         Thread Execute       ResumeThread       0x402409         Check Invalid Close→Exception       CloseHandle       0x402E5D         Check Invalid Close→Exception       CloseHandle       0x402E5D         Check Invalid Close→Exception       CloseHandle       0x402E66         Time Check       GetTickCount       0x402E766         Time Check       GetTickCount       0x402E70         Time Check       GetTickCount       0x402E70         Check Invalid Close→Exception       CloseHandle       0x402E70         Time Check       GetTickCount       0x402E70         Time Check       GetTickCount       0x402E70	Memory Manipulation	VirtualProtectEx	0×4019C7		
Memory Manipulation     VirtualProtectEx     0x4019DD       Memory Manipulation     VirtualProtectEx     0x401A11       Check Invalid Close->Exception     CloseHandle     0x402170       Thread Execute     ResumeThread     0x402170       Time Check     WaitForSingleObject     0x40217E       Thread Manipulation     SuspendThread     0x402203       Time Check     WaitForSingleObject     0x4022D1       Thread Manipulation     SuspendThread     0x4022C3       Time Check     WaitForSingleObject     0x4022D1       Thread Manipulation     SuspendThread     0x4022E4       Thread Execute     ResumeThread     0x40235B       Check Invalid Close->Exception     CloseHandle     0x402409       Check Invalid Close->Exception     CloseHandle     0x402E5D       Check Invalid Close->Exception     CloseHandle     0x402E5D       Check Invalid Close->Exception     CloseHandle     0x402E66       Check Invalid Close->Exception     CloseHandle     0x402E66       Time Check     GetTickCount     0x402F66     Ime Check       Time Check     GetTickCount     0x402F66     Ime Check       Check Invalid Close->Exception     CloseHandle     0x402F66       Time Check     GetTickCount     0x402F66       Check Invalid Close->Exc				Memory_EXECUTE_READWRITE_2	0×4019d1
Memory Manipulation       VirtualProtectEx       0x40111         Check Invalid Close→Exception       CloseHandle       0x402170         Time Check       ResumeThread       0x402170         Time Check       WaitForSingleObject       0x40217E         Thread Manipulation       SuspendThread       0x402191         Thread Execute       ResumeThread       0x402203         Time Check       WaitForSingleObject       0x4022D1         Thread Execute       ResumeThread       0x4022E4         Thread Execute       ResumeThread       0x40235B         Check Invalid Close→Exception       CloseHandle       0x402409         Check Invalid Close→Exception       CloseHandle       0x4022B3         Check Invalid Close→Exception       CloseHandle       0x402E5D         Check Invalid Close→Exception       CloseHandle       0x402E5D         Check Invalid Close→Exception       CloseHandle       0x402E5D         Time Check       GetTickCount       0x402E60         Time Check       GetTickCount       0x402E66         Time Check       GetTickCount       0x402F66         Time Check       GetTickCount       0x402F66         Time Check       GetTickCount       0x402F66         Time Check	Memory Manipulation	VirtualProtectEx	0×4019DD		
Check Invalid Close→Exception CloseHandle 0x401255 Thread Execute ResumeThread 0x402170 Time Check WaitForSingleObject 0x40217E Thread Manipulation SuspendThread 0x402191 Thread Execute ResumeThread 0x402203 Time Check WaitForSingleObject 0x4022D1 Thread Execute ResumeThread 0x4022E4 Thread Execute ResumeThread 0x402258 Check Invalid Close→Exception CloseHandle 0x402409 Check Invalid Close→Exception CloseHandle 0x402E50 Check Invalid Close→Exception CloseHandle 0x402E50 Check Invalid Close→Exception CloseHandle 0x402E50 Time Check GetTickCount 0x402F60 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x4022F6	Memory Manipulation	VirtualProtectEx	0×401 A11		
Thread Execute ResumeThread 0x402170 Time Check WaitForSingleObject 0x40217E Thread Manipulation SuspendThread 0x402203 Time Check WaitForSingleObject 0x4022C3 Time Check WaitForSingleObject 0x4022D1 Thread Execute ResumeThread 0x4022E4 Thread Execute ResumeThread 0x40225B Check Invalid Close→Exception CloseHandle 0x402409 Check Invalid Close→Exception CloseHandle 0x402403 Check Invalid Close→Exception CloseHandle 0x402E5D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x402E7F	Check Invalid Close->Exception	CloseHandle	0×401 E35		
Time Check WaitForSingleObject 0x40217E Thread Manipulation SuspendThread 0x402191 Thread Execute ResumeThread 0x4022C3 Time Check WaitForSingleObject 0x4022D1 Thread Manipulation SuspendThread 0x4022E4 Thread Execute ResumeThread 0x4022E4 Thread Execute ResumeThread 0x4022E4 Thread Execute ResumeThread 0x4022E4 Check Invalid Close→Exception CloseHandle 0x402409 Check Invalid Close→Exception CloseHandle 0x402E5B Check Invalid Close→Exception CloseHandle 0x402E5D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402F60 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x402E5D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x402F66 Check Invalid Close→Exception CloseHandle 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x403F66 Check Invalid Close→Exception CloseHandle 0x403F60 Che	Thread Execute	ResumeThread	0×402170		
Thread Manipulation SuspendThread 0×402191 Thread Execute ResumeThread 0×4022C3 Time Check WaitForSingleObject 0×4022D1 Thread Manipulation SuspendThread 0×4022E4 Thread Execute ResumeThread 0×40235B Check Invalid Close→Exception CloseHandle 0×402409 Check Invalid Close→Exception CloseHandle 0×402423 Check Invalid Close→Exception CloseHandle 0×402E5D Check Invalid Close→Exception CloseHandle 0×402E5D Time Check GetTickCount 0×402F60 Time Check GetTickCount 0×402F66 Time Check GetTickCount 0×402F66 Check Invalid Close→Exception CloseHandle 0×402F66 Check Invalid Close→Exception CloseHandle 0×402F66 Time Check GetTickCount 0×402F66 Check Invalid Close→Exception CloseHandle 0×402F66	Time Check	WaitForSingleObject	0×40217E		
Thread Execute ResumeThread 0x402203 Time Check WaitForSingleObject 0x4022D1 Thread Manipulation SuspendThread 0x4022E4 Thread Execute ResumeThread 0x40235B Check Invalid Close→Exception CloseHandle 0x402409 Check Invalid Close→Exception CloseHandle 0x402423 Check Invalid Close→Exception CloseHandle 0x402E5D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402F66 Check Invalid Close→Exception CloseHandle 0x402E5D	Thread Manipulation	SuspendThread	0×402191		
Time Check     WaitGorSingleObject     0x4022D1       Thread Manipulation     SuspendThread     0x4022E4       Thread Execute     ResumeThread     0x40235B       Check Invalid Close->Exception     CloseHandle     0x402409       Check Invalid Close->Exception     CloseHandle     0x4022B3       Check Invalid Close->Exception     CloseHandle     0x4022B3       Check Invalid Close->Exception     CloseHandle     0x4022F0       Check Invalid Close->Exception     CloseHandle     0x4022F0       Time Check     GetTickCount     0x402F60       Time Check     GetTickCount     0x402F0F       Check Invalid Close->Exception     CloseHandle     0x402F66       Time Check     GetTickCount     0x402F0F       Check Invalid Close->Exception     CloseHandle     0x402F0F	Thread Execute	ResumeThread	0×4022C3		
Thread Manipulation SuspendThread 0x4022E4 Thread Execute ResumeThread 0x40235B Check Invalid Close→Exception CloseHandle 0x402423 Check Invalid Close→Exception CloseHandle 0x402423 Check Invalid Close→Exception CloseHandle 0x402E5D Check Invalid Close→Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402E66 Time Check GetTickCount 0x402E76 Check Invalid Close→Exception CloseHandle 0x402E76 Check Invalid Close→Exception CloseHandle 0x402E70 Time Check GetTickCount 0x402E76 Check Invalid Close→Exception CloseHandle 0x402E76 Check Invalid Close→Exception CloseHandle 0x402E76 Time Check GetTickCount 0x402E76 Check Invalid Close→Exception CloseHandle 0x402E	Time Check	WaitForSingleObject	0×4022D1		
Thread Execute ResumeThread 0x40235B Check Invalid Close->Exception CloseHandle 0x402409 Check Invalid Close->Exception CloseHandle 0x402423 Check Invalid Close->Exception CloseHandle 0x402EB3 Check Invalid Close->Exception CloseHandle 0x402E5D Time Check GetTickCount 0x402E60 Time Check GetTickCount 0x402E66 Time Check GetTickCount 0x402F66 Check Invalid Close->Exception CloseHandle 0x402EFC Check Invalid Close->Exception CloseHandle 0x402E5D	Thread Manipulation	SuspendThread	0×4022E4		
Check Invalid Close->Exception CloseHandle       0x402409         Check Invalid Close->Exception CloseHandle       0x402423         Check Invalid Close->Exception CloseHandle       0x402BB3         Check Invalid Close->Exception CloseHandle       0x402E5D         Time Check       GetTickCount         0x402F66       0x402F66         Time Check       GetTickCount         0x402F6F       0x402F66         Check Invalid Close->Exception CloseHandle       0x402F66	Thread Execute	ResumeThread	0×40235B		
Check Invalid Close->Exception CloseHandle     0x402423       Check Invalid Close->Exception CloseHandle     0x402BB3       Check Invalid Close->Exception CloseHandle     0x402E5D       Time Check     GetTickCount       0x402F60       Time Check     GetTickCount       0x402F0F       Check Invalid Close->Exception CloseHandle       0x402F60       Time Check       GetTickCount       0x402F0F       Check Invalid Close->Exception CloseHandle       0x402F6F       Check Invalid Close->Exception CloseHandle       0x403F0F	Check Invalid Close->Exception	CloseHandle	0×402409		
Opened_Exclusively_Check     0x402b79       Check Invalid Close->Exception CloseHandle     0x402B53     0x402E5D       Check Invalid Close->Exception CloseHandle     0x402E5D     0x402E5D       Time Check     GetTickCount     0x402F60       Time Check     GetTickCount     0x402F66       Time Check     GetTickCount     0x402F6F       Check Invalid Close->Exception CloseHandle     0x40364D	Check Invalid Close->Exception	CloseHandle	0×402423		
Check Invalid Close->Exception CloseHandle     0x402BB3       Check Invalid Close->Exception CloseHandle     0x402E5D       Time Check     GetTickCount     0x402F60       Time Check     GetTickCount     0x402E766       Time Check     GetTickCount     0x402E76       Check Invalid Close->Exception CloseHandle     0x402E76       Check Invalid Close->Exception CloseHandle     0x40364D				Opened_Exclusively_Check	0×402b79
Check Invalid Close->Exception CloseHandle     0x402E5D       Time Check     GetTickCount     0x402F60       Time Check     GetTickCount     0x402F66       Time Check     GetTickCount     0x402F05       Check Invalid Close->Exception CloseHandle     0x40364D	Check Invalid Close->Exception	CloseHandle	0×402BB3		
Time Check         GetTickCount         0x402F60           Time Check         GetTickCount         0x402F66           Time Check         GetTickCount         0x402F0           Check Invalid Close->Exception CloseHandle         0x40364D	Check Invalid Close->Exception	CloseHandle	0×402E5D		
Time Check GetTickCount 0x402F66 Time Check GetTickCount 0x402FCF Check Invalid Close−>Exception CloseHandle 0x40364D	Time Check	GetTickCount	0×402F60		
Time Check GetTickCount 0x402FCF Check Invalid Close->Exception CloseHandle 0x40364D	Time Check	GetTickCount	0×402F66		
Check Invalid Close->Exception CloseHandle 0x40364D	Time Check	GetTickCount	0×402FCF		
	Check Invalid Close->Exception	CloseHandle	0×40364D		

Figure 6: Screen of Anti Debug Detection Results tab.

The column structure of Anti Debug Detection Results is as follows:

- Category Name API category name defined in the Anti\_Debug\_API as listed in anti\_debug.config.
- Possible Anti-Debug API List of detected APIs displayed.
- Address Address where the detected API is being used.
- Possible Anti-Debug Technique Detection name identified by the keyword defined in Anti Debug Technique as listed in anti debug.config.

• Address

Address of the first detected keyword.

Address Transition

By double-clicking on the detected line, you will jump to the address specified.

After running the plugin, detected APIs and keywords are highlighted in different colours.

Detection Category	Color
Anti_Debug_API	Green
Anti_Debug_Technique	Orange

Figure 7: Differences in colour by category.

Furthermore, should an API detailed within the Anti\_Debug\_API section be identified, the corresponding category name is annotated as a comment (Figure 8). Similarly, upon detection of a rule name within the Anti\_Debug\_Technique section, a commentary derived from the JSON file illustrated in Figure 5 is appended as a note to the initially detected keyword (Figure 9).

call	sub_401D30
mov	ds:WriteProcessMemory, eax ; Write Data OnTheMemory
mov	edx, 9D00A761h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:ReadProcessMemory, eax ; MemoryRead,ProcessInspection
mov	edx, 9ABFB8A6h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:VirtualAllocEx, eax ; Memory Manipulation
mov	edx, 6B416786h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:GetCurrentProcessId, eax
mov	edx, 774393E8h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:GetModuleFileNameA, eax
mov	edx, 2EE4F10Dh
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:CopyFileA, eax
mov	edx, 19F78C90h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:Process32First, eax ; Process Check
mov	edx, 0D89AD05h
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:GetCurrentProcess, eax
mov	edx, 0C930EA1Eh
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:Process32Next, eax ; Process Check
mov	edx, SBC1014rn
mov	eax, [ebp+var_8]
call	sub_401D30
mov	ds:Createrooinelp32Snapshot, eax ; Process Check
Imov	POX //(U95b/D

Figure 8: Detected in the Anti\_Debug\_API section.

push	ebo
mov	ebo, eso
and	esp. dFFFFFF8h
mov	eav. Jarge fs:30h : NtGlobalElag check - The code is checking the NtGlobalElag value at offset 0x68 from the Process Environment Block
	The value 70 is the sum of FIG HEAD FMARIE TATI CHECK (0x10) FIG HEAD FMARIE FDFF (HECK (0x20) and FIG HEAD VALIDATE DADAMETERS (0x40)
sub	
test	byte ntr [eav+68h] 70h
nuch	ari
push	adi
17	chart loc 4RFFR2
J4	
mov	[ebp+Context-ContextFlags], 10010h; Hardware_Breakpoints_Check - Check the debug registers DR0, DR1, DR2, and DR3 (CONTEXT_DEBUG_REGISTERS 0x10010); to determine if a hardware breakpoint has been set.
lea	eax, [ebp+Context]
push	eax : lpContext
call	ds:GetCurrentThread
push	eax : hThread
call	ds:GetThreadContext : Thread Manipulation
mov	ecx. [ebp+var 4]
xor	Pax Pax
vor	ery ehn · Starkfookje
ca11	A security check cookie(4) - security check cookie(x)
mov	esn ahn
nov	aba
pop	eop
rech	anda
-marn	enup
<u> </u>	
push	ebp
mov	ebp, esp
push	ecx
mov	eax, large 1s:300; BeingDebugged_check - The BeingDebugged field in the Process Environment Block (PEB) indicates whether the current process is being debugged or not
movzx	cax, byte ptr [cax12]
test	eax, eax
setnz	byte ptr [ebprvar]+j
Cmp	
jz	short loc_40102E

Figure 9: Detected in the Anti\_Debug\_Technique section.

Upon initiating the plugin using the Ctrl+Shift+D shortcut, the system not only presents the anti-debug detection results but also includes a newly added feature that displays a list of detected functions. From the perspectives of the anti-debug detection results and the detected function list, there is an enhanced understanding of both the detection outcomes and the overarching code structure. Concurrently, the debugging process is streamlined by systematically organizing information by function. Collectively, these windows support a dual-perspective approach to malware analysis.

Below is a list of the basic features of the Detected Function List:

- Display the anti-debug detection results, organized by function.
- For items detected by the rules in the Anti\_Debug\_Technique section, displayed in pink text, the rule descriptions can be viewed by hovering over them with the mouse.
- Clicking on the areas highlighted in yellow under the function names will navigate to those addresses.
- Entering text in the search bar initiates a search, and matching results are highlighted in blue.



Figure 10: Screen of Detected Function List – basic functions.

The Detected Function List, in addition to its basic features, displays the hierarchical structure of where detected functions are being called from when function names starting with 'Sub' are double-clicked. In the hierarchical display, function names include 'depth:[number]' to indicate their depth from the Original Entry Point. If the text is in grey, it indicates that the function has been detected in the Anti Debug Detection Lists. Furthermore, double-clicking on the displayed function names navigates to the address where that function is called.



Figure 11: Screen of Detected Function List – recursive checking.

#### List of detectable anti-debugging techniques (all 47 rules)

VMware_I/O_port	NtGlobalFlag_check	Memory_Region_Tracking
VMware_magic_value	NtGlobalFlag_check_2	Check_BreakPoint_Memory_1

HeapTailMarker	HeapFlags	Check_BreakPoint_Memory_2
KernelDebuggerMarker	HeapForceFlags	Software_Breakpoints_Check
DbgBreakPoint_RET	Combination_of_HEAP_Flags	Hardware_Breakpoints_Check
DbgUiRemoteBreakin_Debugger_Terminate	Combination_of_HEAP_Flags_2	ChildProcess_Check
PMCCheck_RDPMC	ReadHeapFlags	Enumerate_Running_Processes
TimingCheck_RDTSC	ReadHeapFlags_2	ThreadHideFromDebugger
SkipPrefixes_INT1	DebugPrivileges_Check	NtQueryInformationProcess_PDPort
INT2D_interrupt_check	CreateMutex_AlreadyExist	NtQueryInformationProcess_PDFlags
INT3_interrupt_check	CreateEvent_AlreadyExist	$NtQueryInformation Process\_PDObjectHandle$
EXCEPTION_BREAKPOINT	Opened_Exclusively_Check	NtQuerySystemInformation_KD_Check
ICE_interrupt_check	$EXCEPTION\_INVALID\_HANDLE\_1$	Extract_Resource_Section
DBG_PRINTEXCEPTION_C	$EXCEPTION\_INVALID\_HANDLE\_2$	Commucate_function_String
TrapFlag_SingleStepException	$Memory\_EXECUTE\_READWRITE\_1$	Commucate_function
BeingDebugged_check	Memory_EXECUTE_READWRITE_2	

# ANTIDEBUGSEEKER FOR GHIDRA

The basic search logic is the same across the versions for IDA and Ghidra.

# Files required to run the program

- AntiDebugSeeker.java (for Ghidra script version)
- Zip folder containing the compiled files: ghidra\_11.0.1\_AntiDebugSeeker.zip (for Ghidra module extension)
- anti\_debug\_Ghidra.config (converted for Ghidra: a file containing rules for detecting anti-debugging techniques)
- anti\_debug\_technique\_descriptions\_Ghidra.json (converted for Ghidra: a file containing descriptions of the detected rules)

# How to run in the Ghidra scrip version

When utilizing Ghidra Script, one can select AntiDebugSeeker.java from the Script Manager and proceed to execute it.



Figure 12: How to run in the Ghidra script version.

When the script is initiated, a prompt entitled 'Select the Configuration File' appears. Users are required to specify the anti\_debug\_Ghidra.config, which defines the detection rules, before selecting 'Open' to proceed.

🧖 Select the Configurat	tion File			×
🗢 🔿 🕆 🔀 🗘	ihatu¥Desktop¥AntiDebugSeeker_Files	- 5	6	3
My Computer	Jebug_Ghidra.config Jebug_techniques_descriptions_Ghidra.json			
File name	anti_debug_Ghidra.config			
Туре:	All Files (**)			<u> </u>
	Open Cancel			

Figure 13: Select the configuration file, anti\_debug\_Ghidra.config.

Following the selection of the configuration file, a prompt titled 'Select the JSON Description File' appears. Users are required to specify the anti\_debug\_technique\_descriptions\_Ghidra.json file, which contains the descriptions of the detection rules, and then click 'Open' to continue.

A Select the JSON Description File			×
← ⇒ ↑ C¥Users¥kaihatu¥Desktop¥AntiDebugSeeker_Files	5	6	a,
My Computer   Work   Desktop     Nome   Nome   Nome   Nome   Nome   Nome     Nome <td></td> <td></td> <td></td>			
File name: anti_debug_techniques_descriptions_Ghidra,ison			
Type:   All Files (**)			<u> </u>
Open Cancel			

Figure 14: Select the description file, anti\_debug\_technique\_descriptions\_Ghidra.json.

#### How to set up and execute the Ghidra module extension

To integrate and operate the module version of AntiDebugSeeker within Ghidra, rather than utilizing a script, the following steps are necessary. The module version features a graphical user interface, which facilitates a visual comprehension of the analysis results, and is therefore recommended.

- 1. Select the file > Install Extensions
- Click + button, then Select Install Extensions. (ghidra\_11.0.1\_PUBLIC\_AntiDebugSeeker.zip) After Opening CodeBrowser
- 3. Select the file.
- 4. In the Configure menu, check 'Examples.
- 5. Click 'Configure,' select 'AntiDebugSeekerPlugin,' and click 'OK.

First, prior to launching Ghidra's CodeBrowser, we will proceed with the steps necessary to install the AntiDebugSeeker plugin.

Help
C 1 11
Ctrl+N
Ctrl+O
•
Ctrl+W
Ctrl+S
1
Ctrl+I
Ctrl+Q

Figure 15: Select File > Install Extensions.

	Marria	1	) (***		-		
DO: 51 /	Name	Description				sion	
BaimElastic	Plugin	n Elastic search backend for BSim.					
Machinel.on	mbler		Endo functiona uning MI	11.0.1			
cample	riirig		Sample code for extension developers	11.0.1			
SampleTable	Plugin		Sample plugin for creating and manipulating a table	11.0.1			
SleighDevTo	nls		Sleigh language development tools including external disas	11.0.1			
Select Ex	tension						×
			AntiDebugSeeker¥dist		- 🧙 🖪		4
							_
	ghidra_	11.0.1_Antil	UebugSeeker zip				
<u> </u>							
My Computer							
~							
Desktop							
Desktop							
Desktop							
Desktop							
Desktop Home							
Desktop Home							
Desktop Home							
Desktop Home							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Mome Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desktop Home Recent							
Desk top Home Recent							
Desktop Mome Recent							
Desktop Toesktop Home							
Desktop Tome Home Recent	File name:	ehidra 110	11 AntiDebugSeeker z io				

Figure 16: Install a ZIP file (compiled AntiDebugSeeker).

File Edit Analysis Graph Navigation Open Close 0000000 dump 2 SCV eve Close File > CC Save A Save 1 Save 1	Search S Ctrl+0 Ctrl+W Dnfig Check	ure > ( AntiD	Check Examp ebugSeekerP	oles > Click Configure Plugin > Click Ok
Import File Batch Import	R 🄇	Ghidra Core <u>Configure</u>	These plugins provide that basic set of reverse en	Invertie capabilities
Open File System Add To Program	n 🌒	BSim Configure	An API and sat of plugins for creating, managing an similarity	AntCebusSeekerFlugh     Use AntCebusSeekerFlugh in Ohids     Analysis
Export Program Load PDB File	- <b>#</b>	Debugger Configure	Plugins for debugging and tracing	
Parse C Source Print	- <b>6</b>	Miscellaneous Configure	These plugins do not belong to a package	
Page Setup Configure	n 🤌	Developer Configure	These plugins provide features useful for developin	
Save Tool Save Tool As	₽ 🗸	Examples Configure	These plugins are just examples of how to write a p	
Export Close Tool	п 🛓	Experimental Configure	This package contains plugins that are not fully tes documented You must add these plugins individually could cause the tool to become unstable.	Film: 0 # *
Exit Ghidra			Close	
Filter:	2	Analysis Analysis Analysis Analysis Analysis Analysis Analysis		<]>

Figure 17: How to integrate the module version of AntiDebugSeeker.

After integration, 'AntiDebugSeekerPlugin' will be available in the Window menu; users are advised to click on it to continue.

File Edit Analysis Graph Navigation Search	Select Tools	Window Help			
	IDU	AntiDebugSeekerPlugin		🖄 🖽 🖻 🔓 🚠 🔿 🛛	I 🔶 🔲 🖪 🐣 🛛 🌒
		V Bookmarks	Ctrl+B		
Program Trees	E Listing:	Bundle Manager			
E _ 00120000_dump_2_SCY.exe		Bytes: 00120000 dump 2 SCY.exe			
Headers		Checksum Generator			
CODE		Comments		00-ram:00400311	
idata		Data Type Manager			
- Filoc		Data Type Preview		DER_00400000	XREF[1]
irsrc isrc		Ct Decompiler UndefinedEunction 00/1260	0 Ctrl+E		
SCY SCY		101 Defined Data	o cui+c		
		0101 Defined Strings			
		Dat Denned Strings		[] "MZ"	e_magic
		Exusted Table		500	e chin
		Equates Table		2h	e cp
		External Programs		Oh	e crlc
		Function Call Graph		4h	e_cparhdr
Program Tree ×		Superior Call Trees		Fh	e_minalloc
	1	Function Graph		FFFFh	e_maxalloc
		Function Tags		Oh	e_ss
E Exports		Functions		B8h	e_sp
Functions		Listing: _00120000_dump_2_SCY.exe		On	e_csum
🕀 📴 Labels	🖌 Bookmar	🛄 Memory Map			
E Classes		Program Trees		<b>B</b>	Category
	Analysis	🗬 Python		Found Code	
	Analysis	🔶 Register Manager		Found Code	
	Analysis	Relocation Table		Found Code	
	Analysis	Script Manager		Found Code	
	Analysis	Symbol References		Found Code	
	Analysis	Symbol Table	Ctrl+T	Found Code	
	Analysis	Symbol Tree		Found Code	
	Analysis			Found Code	
	Analysis			Found Code	

Figure 18: Select AntiDebugSeekerPlugin from the Window tab.

When the plugin is launched, as illustrated in Figure 19, three clickable buttons are available: 'Start Analyze', 'Display Only the Detection Results' and 'Detected Function List'. Clicking the 'Start Analyze' button loads the configuration and JSON files and initiates the analysis.

Antibudesele Pugn	×
Start Analyze ] Display only the detection results Detected Function List	

Figure 19: Startup screen.

A screen with a small dragon and file selection options will appear. 'Select Config File' is displayed. Specify the anti\_debug\_Ghidra.config file that defines the detection rules, and then click 'Open'.

Look ir	n: 📙 AntiDebu	gSeeker_Files	•	<del>ئ</del> 😕 ⊅	
€ 最近使った項…	🗭 anti_debu	ıg_Ghidra.config			
デスクトップ					
الم المراجع المراجع					
PC					
٢	, File name:	anti_debug_Ghidra.config			Open
	Look ir 最近使った項 デスクトップ ドキュメント PO	Look in: AntiDebu 最近使った項 デスクトップ ドキュメント PC File name:	Look in: AntiDebugSeeker_Files	Look ir: AntiDebugSeeker_Files AntiDebugSeeker_Files Anti_debug_Ghidra.config Anti_debug_Ghidra.config File name: anti_debug_Ghidra.config	Look in: AntiDebugSeeker_Files   Anti_debug_Ghidra.config  Anti_debug_Ghidra.config  File name: anti_debug_Ghidra.config  File name: anti_debug_Ghidra.config

Figure 20: Select the config file.

Similar to the Ghidra script version, a prompt to 'Select JSON File' will be displayed. Specify the anti\_debug\_technique\_ descriptions\_Ghidra.json file, which contains the descriptions of the detection rules, and then click 'Open'.

Look in:	AntiDebu	ugSeeker_Files	~	🤌 📂 🛄-	
最近使った項 デスクトップ ドキュメント	anti_debu	ug_techniques_descriptions_Ghidrajson			
¥ ¢-⊂بر≮	File name: Files of type:	anti_debug_techniques_descriptions_Ghidra	ijson		Open Cancel



# **VERIFYING THE RESULTS, GHIDRA SCRIPT + MODULE EXTENSION**

#### Ghidra script: check console-scripting

The results of the detection can be reviewed from the Console - Scripting screen. The message 'AntiDebugSeeker Process Finished' indicates that the process has successfully completed.

🖳 Console – Scripting	
AntiDebugSeeker.java> Running	
AntiDebugSeeker.java> Start AntiDebugSeeker Script .	
AntiDebugSeeker.java> IsDebuggerPresent API not found	d.
AntiDebugSeeker.java> OutputDebugStringA API not four	nd.
AntiDebugSeeker.java> OutputDebugStringW API not four	nd.
AntiDebugSeeker.java> CreateToolhelp32Snapshot API no	ot found.
AntiDebugSeeker.java> GetWindowThreadProcessId API no	ot found.
AntiDebugSeeker.java> NtQueryInformationProcess API :	not found.
AntiDebugSeeker.java> Process32First API not found.	
AntiDebugSeeker.java> Process32Next API not found.	🖳 Console – Scripting
AntiDebugSeeker.java> MapViewOfFile API found.	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00402530
AntiDebugSeeker.java> 0040775f	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00402540
AntiDebugSeeker.java> UnmapViewOfFile API found.	AntiDebugSeeker.java> Found Single keyword Rule'http' at 0040264c
AntiDebugSeeker.java> 00407606	AntiDebugSeeker.java> Found Single keyword Rule'http://at/00402654
AntiDebugSeeker.java> VirtualAlloc API found.	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00402664
AntiDebugSeeker.java> 0040204a	AntiDebugSeeker.java> Found Single keyword Rule'http' at 0040a935
AntiDebugSeeker.java> 004016a9	AntiDebugSeeker.java> Found Single keyword Rule'http' at 0040a97b
AntiDebugSeeker.java> VirtualAllocEx API not found.	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00411c31
AntiDebugSeeker.java> VirtualProtect API found.	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00411c57
AntiDebugSeeker.java> 00402035	AntiDebugSeeker.java> Found Single keyword Rule'http:/ at 004131cd
AntiDebugSeeker.java> 00402099	AntiDebugSeeker.java> Found Single keyword Rule'http' at 004131ea
AntiDebugSeeker.java> 00402155	Antibebugdeeker, java- Found Single keyword Rule http://at.00413669
AntiDebugSeeker.java> 004021bf	AntiDebugSeeker.java> Found Single keyword Rule'http' at 004193f8
AntiDebugSeeker.java> 00414dd6	AntiDebugSeeker.java> Found Single keyword Rule'http' at 004193fc
	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00419454
	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00419458
	AntiDebugSeeker.java> Found Single keyword Rule'http' at 00419494
	AntiDebugSeeker.java> Found Single keyword Rule'http://at/0019498
	AntiDebugSeeker.java> AntiDebugSeeker Process Finished
	AntiDebugSeeker.java> *** Please Check the Results from Bookmarks
	AntiDebugSeeker.java> Finished!

Figure 22: Script analysis completion screen.

#### Ghidra module extension: check text area

When the analysis is complete, 'Analysis Complete' will be displayed. Monitor the progress on the right side of the screen using the progress bar. Once the bar reaches 100%, the analysis is complete. On the displayed screen, you can review both the detected and undetected items. At this point, the results are already registered in Ghidra's Bookmark feature.



Figure 23: Plugin analysis completion screen.

Upon detection by Anti\_Debug\_Technique, the system will display the name of the detection rule, the position of the detected keyword within the rule, and the address where the detection occurred.

Keyword group Memory_EXECUTE_READWRITE_1 found starting at: 0040203f in direct search. In function FUN_00402004
Detected Second Keyword is 00402041
Detected Third Keyword is 0040204a
Searching for keyword group: Memory_EXECUTE_READWRITE_2 with search range: 20
Keyword group Memory_EXECUTE_READWRITE_2 found starting at: 0040202d in direct search. In function FUN_00402004
Detected Second Keyword is 00402035
Keyword group Memory_EXECUTE_READWRITE_2 found starting at: 0040214d in direct search. In function FUN_00402114
Detected Second Reyword is 00402155
Keyword group Memory_EXECUTE_READWRITE_2 found starting at: 00414dc2 in direct search. In function entry
Detected Second Reyword is 00414dd6
Searching for keyword group: Memory_Region_Tracking with search range: 250
Searching for keyword group: Check_BreakPoint_Memory_1 with search range: 80
Searching for keyword group: Check_BreakPoint_Memory_2 with search range: 80
Searching for keyword group: Software_Breakpoints_Check with search range: 300
Searching for keyword group: Hardware_Breakpoints_Check with search range: 80
Searching for keyword group: Enumerate_Running_Processes with search range: 250
Keyword group Enumerate_Running_Processes found starting at: 00402f62 in direct search. In function FUN_00402c74
Detected Second Keyword is 00402f86

Figure 24: Display when detected by the rules specified in Anti\_Debug\_Technique.

Clicking the 'Display only the detection results' button, as shown in Figures 25 and 26, displays only the detected items, making it easy to review the results.

😤 AntiDebugSeelerPlugin			
	Start Analyze	Display only the detection results	Detected Function List
IsDebuggerPresent API not found.			
OutputDebugStringA API not found.			
OutputDebugStringW API not found.			
CreateToolhelp32Snapshot API not found.			
GetWindowThreadProcessId API not found.			
NtQueryInformationProcess API not found.			
Process32First API not found.			
Process32Next API not found.			
MapViewOfFile API found.			
0040775f in function FUN_004076f8			
UnmapViewOfFile API found.			
00407606 in function FUN_004075dc			
VirtualAlloc API found.			
0040204a in function FUN_00402004			
004016a9 in function FUN_00401690			
VirtualAllocEx API not found.			
VirtualProtect API found.			
00402035 in function FUN_00402004			
00402099 in function FUN_00402004			
00402155 in function FUN_00402114			
004021bf in function FUN_00402114			
00414dd6 in function entry			

Figure 25: Before processing 'Display only the detection results'.

🅵 AntiDebugSeekerPlugin			
	Start Analyze	Display only the detection results	Detected Function List
MapViewOfFile API found.			
0040775f in function FUN_004076f8			
UnmapViewOfFile API found.			
00407606 in function FUN_004075dc			
VirtualAlloc API found.			
0040204a in function FUN_00402004			
004016a9 in function FUN_00401690			
VirtualProtect API found.			
00402035 in function FUN_00402004			
00402099 in function FUN_00402004			
00402155 in function FUN_00402114			
004021bf in function FUN_00402114			
00414dd6 in function entry			
CreateMutexA API found.			
004077f5 in function FUN_004076f8			
004149e0 in function FUN_00414938			
GetComputerNameA API found.			
0040ba6f in function FUN_0040ba4c			
00406443 in function FUN_00406420			
0040657b in function FUN_00406558			
GetSystemTime API found.			
0040a7d2 in function FUN_0040a7c8			
GetTickCount API found.			
0040b8f7 in function FUN_0040b754			
0040b845 in function FUN_0040b754			
00414157 in function FUN_00413eb8			
0040c581 in function FUN_0040c544			
0040c5ec in function FUN 0040c544			

Figure 26: After processing 'Display only the detection results'.

In the states depicted in Figures 25 and 26, before and after processing 'Display only the detection results', clicking the 'Detected Function List' button groups the detection results by function. This organization facilitates a clearer understanding of the anti-debugging features at the function level.

🐕 AntiDebugSeekerPlugin	
	Start Analyze Display only the detection results Detected Function List
FUN_004076f8	
MapViewOfFile : 0040775f	
CreateMutexA : 004077f5	
FUN_004075dc	
UnmapViewOfFile : 00407606	
FUN_00402004	
VirtualAlloc : 0040204a	
VirtualProtect : 00402035	
Memory EXECUTE READWRITE 1 : 0040203f	
Memory EXECUTE READWRITE 2 : 0040202d	
FUN_0040ba4c	
GetComputerNameA : 0040ba6f	
FUN 0040a7c8	
GetSystemTime : 0040a7d2	
FUN_0040b754	
GetTickCount : 0040b8f7	
FUN 004076d8	
WaitForSingleObject : 004076e3	
FUN_0040c614	
CreateThread : 0040c63f	
FUN_00414938	
GetCursorPos : 00414c2c	
FUN_00413254	
CloseHandle : 004132eb	
Opened_Exclusively_Check : 0041326c	
Opened_Exclusively_Check : 0041328e	
FUN_004010b8	
RDTSC : 004010bc	

Figure 27: After processing 'Detected Function List'.

### Ghidra script / module extension: check Bookmarks

In Figures 28 and 29, the detection results are registered in Ghidra's Bookmark, allowing for easy verification. The category labelled 'Potential of Anti Debug API' indicates detections based on the rules specified in the Anti\_Debug\_API section of the anti\_debug\_Ghidra.config file. Similarly, the category labelled 'Anti Debug Technique' signifies detections based on the rules in the Anti\_Debug\_Technique section. Additionally, entries such as 'Second Keyword' or 'Third Keyword' under 'Anti Debug Technique' denote the specific locations where the defined keywords were detected.

🖊 Bookmarks - (159 bookmarks)						
Туре	Category	Description	Location			
Analysis	Potential of Anti Debug API	Memory Manipulation : MapViewOfFile	0040775f			
Analysis	Potential of Anti Debug API	Memory Manipulation : UnmapViewOfFile	00407606			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualAlloc	0040204a			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualAlloc	004016a9			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualProtect	00402035			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualProtect	00402099			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualProtect	00402155			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualProtect	004021 bf			
Analysis	Potential of Anti Debug API	Memory Manipulation : VirtualProtect	0041 4dd6			
Analysis	Potential of Anti Debug API	Mutual Exclusion : CreateMutexA	004077f5			
Analysis	Potential of Anti Debug API	Mutual Exclusion : CreateMutexA	0041 49e0			
Analysis	Potential of Anti Debug API	Analysis Environment Check : GetComputerNameA	0040ba6f			
Analysis	Potential of Anti Debug API	Analysis Environment Check : GetComputerNameA	00406443			
Analysis	Potential of Anti Debug API	Analysis Environment Check : GetComputerNameA	0040657b			
Analysis	Potential of Anti Debug API	Time Check : GetSystemTime	0040a7d2			
Analysis	Potential of Anti Debug API	Time Check : GetTickCount	0040b8f7			
Analysis	Potential of Anti Debug API	Time Check : GetTickCount	0040b845			
Analysis	Potential of Anti Debug API	Time Check : GetTickCount	00414157			
Analysis	Potential of Anti Debug API	Time Check : GetTickCount	0040c581			
Analysis	Potential of Anti Debug API	Time Check : GetTickCount	0040c5ec			
Analysis	Potential of Anti Debug API	Time Check : WaitForSingleObject	004076e3			
Analysis	Potential of Anti Debug API	Time Check : WaitForSingleObject	004070ea			
Analysis	Potential of Anti Debug API	Time Check : WaitForSingleObject	00413942			
Analysis	Potential of Anti Debug API	Time Check : WaitForSingleObject	00406f20			
Analysis	Potential of Anti Debug API	Time Check : WaitForSingleObject	0041 0e1 6			

Figure 28: After processing 'Detected Function List'.

#### AUTOMATICALLY DETECT AND SUPPORT AGAINST ANTI-DEBUG WITH IDA/GHIDRA... TAKEDA

🥖 Bookmarks - (159 bookmarks)						
	Туре	A	Category	Description	Location	
Analysis		Ar	ti Debug Technique	TimingCheck_RDTSC	00401 0bc	
Analysis		Ar	ti Debug Technique	Opened_Exclusively_Check	00406188	
Analysis		Se	cond Keyword	It was detected at	00406191	
Analysis		Ar	ti Debug Technique	Opened_Exclusively_Check	004061aa	
Analysis		Se	cond Keyword	It was detected at	004061 b3	
Analysis		Ar	ti Debug Technique	Opened_Exclusively_Check	0040c9e3	
Analysis		Se	cond Keyword	It was detected at	0040c9ec	
Analysis		Ar	ti Debug Technique	Opened_Exclusively_Check	0041326c	
Analysis		Se	cond Keyword	It was detected at	00413275	
Analysis		Ar	ti Debug Technique	Opened_Exclusively_Check	0041328e	
Analysis		Se	cond Keyword	It was detected at	00413297	
Analysis		Ar	ti Debug Technique	Memory_EXECUTE_READWRITE_1	0040203f	
Analysis		Se	cond Keyword	It was detected at	00402041	
Analysis		Th	ird Keyword	It was detected at	0040204a	
Analysis		Ar	ti Debug Technique	Memory_EXECUTE_READMRITE_2	0040202d	
Analysis		Se	cond Keyword	It was detected at	00402035	
Analysis		Ar	ti Debug Technique	Memory_EXECUTE_READMRITE_2	0040214d	
Analysis		Se	cond Keyword	It was detected at	00402155	
Analysis		Ar	ti Debug Technique	Memory_EXECUTE_READWRITE_2	0041 4dc2	
Analysis		Se	cond Keyword	It was detected at	0041 4dd6	
Analysis		Ar	ti Debug Technique	Enumerate_Running_Processes	00402f62	
Analysis		Se	cond Keyword	It was detected at	00402f86	
Analysis		Ar	ti Debug Technique	Enumerate_Running_Processes	0041 d1 a0	
Analysis		Se	cond Keyword	It was detected at	0041 d1 a8	

Figure 29: After processing 'Detected Function List'.

Items detected by the Anti Debug API are highlighted with a green background, and the rule name is annotated as a PRE comment.



Figure 30: Disassembly screen showing detections from the Anti\_Debug\_API section of anti\_debug\_Ghidra.config.

Items detected by the Anti Debug Technique are highlighted with an orange background, and the rule name is annotated as a PRE comment. The details of the rule are displayed as a POST comment, derived from the data in the loaded JSON file.

📕 Listing: _001200	100_dump_2_SCY.exe								
	00402000 /4 04	02	280_00402000						
	Memory_EXECUTE_READWRITE_1								
	0040203f 6a 40	PUSH	0x40	; DWORD flProtect for VirtualAlloc					
	First Keyword	he flProtec	t parameter of VirtualAlloc is set to PAGE EXECUT.						
	This enables dynamic writing and execution of new code in the								
	00402041 68 00 30	PUSH	0x3000	: DWORD flallocationType for Vir					
T i									
	Second Keyword	DITCH	0=10	· CITE T duffing for Winter 1311					
		PUSH	0x40	; SIZE_I dwSIZE FOR VIRCUALATIOC					
	UU4U2U48 6a UO PUSH		0x0	; LPVOID 1pAddress for VirtualA1					
	Memory Manipulation								
	0040204a ff 15 ec	CALL	dword ptr [->KERNEL32.DLL::VirtualAlloc]						
	Third Keyword								
		MOV	dword ptr [EBP + local_20],param_1						
	00402053 8b 45 e0	MOV	param 1, dword ptr [EBP + local 24]						
->	00402056 8b 55 e4	MOV	param 2.dword ptr [EBP + local 20]						
*	00403050 00 03	MOLT	durand man forence 01 menore 1						
Dealementer - (16	64 heatmarks)								
DOOK marks - (10	04 DOOKmarks)								
Туре	Category		Description	Location	Label				
Analysis	Potential of Anti Debug API		Check Invalid Close->Exception : CloseHandle	0041288c					
Analysis	Potential of Anti Debug API		Check Invalid Close->Exception : CloseHandle	00414cd2					
Analysis	Anti Debug Technique		TimingCheck_RDTSC	004010bc					
Analysis	Anti Debug Technique		Opened_Exclusively_Check	00406188					
Analysis	Second Keyword		It was detected at	00406191					
Analysis	Anti Debug Technique		Opened_Exclusively_Check	004061aa					
Analysis	Second Keyword		It was detected at	004061b3					
Analysis	Anti Debug Technique		Opened_Exclusively_Check	0040c9e3					
Analysis	Second Keyword		It was detected at	0040c9ec					
Analysis	Anti Debug Techniq	ue	Opened_Exclusively_Check	0041326c					
Analysis	Second Keyword		It was detected at	00413275					
Analysis	Anti Debug Techniq	ue	Opened_Exclusively_Check	0041328e					
Analysis	Second Keyword		It was detected at	00413297					
Analysis	Anti Debug Techniq	ue	Memory_EXECUTE_READWRITE_1	0040203f					
Analysis	Second Keyword		It was detected at	00402041					
Analysis	Third Keyword		It was detected at	0040204a					
Analysis	Anti Debug Techniq	Jê	Memory_EXECUTE_READWRITE_2	0040202d					
Analysis	Second Keyword		It was detected at	00402035					
Analysis	Anti Debug Technique		Memory_EXECUTE_READWRITE_2	0040214d					
Analysis	Second Keyword		It was detected at	00402155					
Analysis	Anti Debug Technique		Memory_EXECUTE_READWRITE_2	00414dc2					
Analysis	Second Keyword		It was detected at	00414dd6					
Analysis	Anti Debug Techniq	ue	Enumerate_Running_Processes	00402f62					
Analysis	Second Keyword		It was detected at	00402f86					

Figure 31: Disassembly screen showing detections from the Anti\_Debug\_Technique section of anti\_debug\_Ghidra.config.

### CONCLUSION

AntiDebugSeeker is a tool designed to automatically detect and analyse anti-debugging features commonly found in malware. For those who have little experience in analysing anti-debugging malware and find it challenging, the detailed descriptions of the rules in the JSON file can serve as a valuable reference. While this tool specializes in detecting anti-debugging techniques, it also highlights common malware techniques through its detection rules. To make this tool accessible to a broader audience, versions have been developed for both IDA and Ghidra. The functional differences between the IDA and Ghidra versions are minimal, allowing users to choose the version that best suits their preferences.

I will update this work as promptly as possible upon the discovery of new anti-debugging techniques. Alternatively, if you report a new technique, I will ensure it is incorporated in the updates. Your collaboration in the development of this tool would be greatly appreciated.

# REFERENCES

- [1] IDA\_Plugin\_AntiDebugSeeker. https://github.com/LAC-Japan/IDA\_Plugin\_AntiDebugSeeker.
- [2] Ghidra\_AntiDebugSeeker. https://github.com/LAC-Japan/Ghidra\_AntiDebugSeeker.