Where is "that" anti-debug? Introduction Of AntiDebugSeeker

Takahiro Takeda







Takahiro Takeda

Malware Analysis Team Cyber Emergency Center LAC

2016: Analysis work as a Security Analyst at JSOC.

2017: Analyzing malware and logs, as well as investigating smishing, at the Japan Cyber Crime Control Center (JC3).

2019: Responsible for malware analysis related to incidents at the Cyber Emergency Center.

Speaker Experience: 2020: PACSEC. 2020: AVAR (Association of Anti-Virus Asia Researchers). 2021: HITCON.

Agenda

- **1.** Introduction of the AntiDebugSeeker
- 2. Demonstration: Using IDA
- **3.** Future Work

Introduction of the AntiDebugSeeker



This is a program for automatically identify and extract potential antidebugging techniques used by malware and displaying them in IDA.

The main functionalities of this plugin are as follows:

1.Extraction of APIs that are potentially being used for anti-debugging by the malware.

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.

For packed samples, running this plugin after unpacking and fixing the Import Address Table is more effective.

About 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.

Anti_Debug_API

###Anti_Debug_API###	###Anti_Debug_API###
[Category Name]	[Debugger check]
API1	CheckRemoteDebuggerPresent
ΔΡΙ2	DebugActiveProcess
	DebugBreak DhaSatDahuaEiltanStata
APIS	DbgSetDebugActiveProcess
	IsDebuggerPresent

Anti_Debug_Technique

###Anti Debug Technique### ###Anti Debug Technique### default search range=80

[Rule1]]
ABC -	80bytes
DEF 🗧	
GHI 🤳	oubytes

default search range=80

[NtGloba]	lFlag_	_check
fs:30h		
68h		
70h		

© 2024 LAC Co., Ltd.



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### [Category Name_1] API1 API2 API3 [Category Name_2] API1 API2 API3

•

About Anti_Debug_Technique in anti_debug.config



In this section, you can set up to three keywords (partial match) under a single rule name.

###Anti_Debug_Technique###
Default search range=80



The basic flow of the search is as follows:

First, the search begins with the first keyword. If it is found, the second keyword is then searched for within a specified number of bytes (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

About Anti_Debug_Technique in anti_debug.config



If you want to set a custom search range instead of using the default value, you can specify 'search_range=value' at the end of the keyword you've set. This allows you to change the search range for each rule you've configured.

###Anti_Debug_Technique###
default_search_range=80

[Rule1]

ABC

EFG

HIJ

search_range=50

[Rule2] KLM NOP search_range=200

© 2024 LAC Co., Ltd.

anti_debug.config Editing Feature



Functionality for checking and editing the contents of anti_debug.config. Ctrl + Shift + E (File Editing Feature)

After making changes, click the 'Save' button to save the modifications.

The contents	
###Anti_Debug_API###	
[Debugger check]	
IsDebuggerPresent	
DebugBreak	
OutputDebugStringA	
OutputDebugStringW	
CheckRemoteDebuggerPresent	
DbgSetDebugFilterState	
NtSetDebugriiterState	
NtQueryObject	
NtSystemDebugcontrol	
[Process Check]	
CreateToolhelp32Snapshot	
Process32Next	
GetWindowThreadProcessId	
DebugActiveProcess	
DbgUiDebugActiveProcess	
NtDebugActiveProcess	
NtSetInformationProcess	
NtQuerySystemInformation	
NtQueryInformationProcess	
[Window Name Check]	
FindWindowA	
FindWindowExA	
FindWindowW	
FindWindowExW	
EnumWindows	
EnumThreadWindows	
GetWindow	
GetWindowTextW	

Save

2024 LAC Co., Ltd



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

Detection Category	Color
Anti_Debug_API	Green
Anti_Debug_Technique	Orange

Additionally, if an API specified in Anti_Debug_API is detected, the category name is added as a comment. Likewise, if a rule name is detected in Anti_Debug_Technique, a description of that rule is added as a comment to the first detected keyword.

<pre>call sub_401D30 mov ds:WriteProcessMemory, eax ; Write Data OnTheMemory mov edx, 9000A761h 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, 68416786h mov edx, 56416786h mov edx, 62410780 mov ds:GetCurrentProcessId, eax mov edx, 77439368h mov eax, [ebp+var_8] call sub_401D30 mov eax, [ebp+var_8] call sub_401D30 mov ds:GetCurrentProcessId, eax</pre>	push ebp, mov ebp, esp and esp, 0FFFFFF8h mov eax, large fs:30h; NtGlobalFlag_check - The code is checking the NtGlobalFlag value at offset 0x68 from the Process Environment Block. ; The value 70 is the sum of FLG_HEAP_ENABLE_TAIL_CHECK (0x10), FLG_HEAP_ENABLE_FREE_CHECK (0x20), and FLG_HEAP_VALIDATE_PARAMETERS (0x40). sub esp, 480h test byte ptr [eax+68h], 70h push edi jz short loc_48FFB2 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.	
<pre>call sub_401030 mov ds:GetModuleFileNameA, eax mov edx, 2EE4F100h mov eax, [ebp+var_8] call sub_401030 mov ds:CopyFileA, eax mov edx, 19F78C90h mov edx, 19F78C90h call sub_401030 mov ds:Process32First, eax ; Process Check mov edx, 0089A005h mov eax, [ebp+var_8] call sub_40123</pre>	<pre>call ds:GetCurrentThread push eax ; lpContext call ds:GetCurrentThread push eax ; hThread call ds:GetThreadContext ; Thread Manipulation mov ecx, [ebp+var_4] xor eax, eax xor ecx, edp ; StackCookie call d_scurity_check_cookie@4 ;security_check_cookie(x) mov esp, ebp pop ebp retn _main endp</pre>	
<pre>mov ds:GetCurrentProcess, eax mov edx, 0C930EA1Eh mov eax, [ebp+var_8] call sub_401D30 mov ds:Process32Next, eax ; Process Check mov edx, 58C1D14Fh mov eax, [ebp+var_8] call sub_401D30 call sub_401D30 mov ds:CreateToolhelp32Snapshot, eax ; Process Check mov edx, 77CD9567h</pre>	push ebp mov ebp, esp push ecx mov eax, large fs:30h ; 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 [ebp+var_4] cmp [ebp+var_4], 0 jz short loc_40102E	024 LA



The following Anti Debug Techniques can be detected using AntiDebugSeeker.

HeapTailMarker KernelDebuggerMarker DbgBreakPoint_RET DbgUiRemoteBreakin_Debugger_Terminate PMCCheck_RDPMC TimingCheck_RDTSC SkipPrefixes_INT1 INT2D_interrupt_check INT3_interrupt_check EXCEPTION_BREAKPOINT ICE_interrupt_check DBG PRINTEXCEPTION C TrapFlag_SingleStepException BeingDebugged_check NtGlobalFlag_check NtGlobalFlag_check_2 HeapFlags HeapForceFlags Combination_of_HEAP_Flags Combination_of_HEAP_Flags_2

ReadHeapFlags ReadHeapFlags_2 DebugPrivileges_Check Opened_Exclusively_Check EXCEPTION_INVALID_HANDLE_1 EXCEPTION INVALID HANDLE 2 Memory_EXECUTE_READWRITE_1 Memory_EXECUTE_READWRITE_2 Memory_Region_Tracking Check_BreakPoint_Memory_1 Check BreakPoint Memory 2 Software_Breakpoints_Check Hardware_Breakpoints_Check Enumerate_Running_Processes ThreadHideFromDebugger NtQueryInformationProcess_PDPort NtQueryInformationProcess_PDFlags NtQueryInformationProcess_PDObjectHandle NtQuerySystemInformation_KD_Check © 2024 LAC Co., Ltd.

Updated functions



ÎÂC

Detected Function List

After launching the plugin with Ctrl+Shift+D, in addition to the Anti Debug Detection Results, we have added a feature to display the Detected Function List.

By adding this feature,

With the Anti Debug Detection Results, it becomes easier to grasp both the detection outcomes and the overall flow of the code, while the Detected Function List allows for a more manageable debugging process by providing information organized by each function. This enables malware analysis from two distinct perspectives.

Updated Feature: Detected Function List – Basic Functions



IDA View-A	🗵 📢 Anti Debug Detection Results 🗵 🚺 Detected Function List 🗵 🧿 Hex View-1 🗵 🖪 Structures 🗵 🔃 Enums	Imports	Exports 🔀
resume		 	
	Double-click on a function name starting with 'sub' to investigate it recursively call.	 	
	You can search for results.		^
sub_4019C0			
(0x4019C0)			
VirtualProtectEx			
VirtualProtectEx			
Memory SYECUTE			
(Adetected)	Whe fillew Protect parameter in Virtual Protect is configured with DAGE EVECLITE DEADWRITE (0x40)		
(Hactected)	This configuration permits both dynamic code insertion and execution within the targeted executable memory area.		
sub 401C4A			
(0x401C4A)			
CloseHandle			
(1detected)	Mouse over to see rule evolutions		
	iviouse over to see rule explanations.		
sub_4020B8			
(0x4020B8)			
WaitForSingleObje	ct		
Suspend Thread			
(2detected)			
(Suelected)			
sub 402215			
(0x402215)			
WaitForSingleObje	ct		
SuspendThread			
ResumeThread			
ResumeThread			
(4detected)			
	.text:0040236A ; Attributes: bp-based frame .text:0040236A		
sub_40236A	Double-click to jump .text:0040236A ; int _stdcall sub_40236A(int,		
(0x40236A)	to a section		
CloseHandle	.text:0040236A var_10= dword ptr -10h		
(2detected)	.text:0040236A var_4= byte ptr -4		
(Lancicotted)	.text:0040236A arg_0= dword ptr 8		
sub_402AEA	.text:0040236A		
(0x402AEA)	.text:0040236A push ebp	 	 ~
	.text:0040236D sub esp 14h		

Updated Feature: Detected Function List – Recursive Checking



IDA View-A	The section Results I Les Detected Function List I Hex View-1	A Structures	Enums		Imports		Exports
sume							
	Double-click on a function name st	arting with 'sub' to investigate it recur	rsively call.				
ub_4019C0 Ix4019C0) VirtualProtectEx VirtualProtectEx VirtualProtectEx Memory_EXECUTE_READWRIT 4detected)	TE_2	Double	Help e Clicking on a fund you to recursi	o Informatio ction name ively check	on: starting wit that functic	h 'sub' allc m.	ows
ub_401C4A tx401C4A) CloseHandle detected) ub_402088 tx402088) WaitForSingleObject SuspendThread	uble-clicking on a function name enables you to trace where function is being called from recursively.	e that -unctions displayed	in gray have been	detected i	n		
ResumeThread		the Dete	cted Function List.				
detected)	Check the recursive calls : sub_402215 — C X	'depth: [number]' i	ndicates the dept	h from the			
L 400015	Items in gray indicate functions that match the Detected Function List	Original	Entry Point (OFP)				
10_402215	sub_402215 called_addr (00401408) (depth:5)	Original					
WaitForSingleObject SuspendThread ResumeThread ResumeThread 4detected)	sub_401395 called_addr (0040154A) (depth:4) sub_4014B7 called_addr (004013C) (depth:3) sub_4040EC called_addr (0040190D) (depth:2) sub_401571 called_addr (00401113) (depth:1) sub_402215 called_addr GetCursorInfo, CloseHandle, CloseHandl	jump to the location w called. dle, Opened_Exclusively_Check,	here the function is b	peing	text:00401100 push text:00401101 call text:00401107 mov text:00401107 call text:00401112 push text:00401113 call	esi ds:GetModuleHa dword_407618, ds:GetCommandl eax sub 401571	; 1pModuleName IndleA eax .ineW
	I sub_40236A_called_addr (0040153E) (depth:4)			•	text:00401118 push	hHeap esi, eax	; hHeap
b_40236A					text:00401120 call	ds:HeapDestroy	r
CloseHandle	Mouse over to see the	function's detection	n results from the				
CloseHandle	Wouse over to see the						
detected)	Dete	ected Function List.					
ib_402AEA							

Demo : AntiDebugSeeker





- Malware : Ursnif
 - MD5: 4da11c829f8fea1b690f317837af8387 (Packed)
 MD5: 952d604345e051fce76729ccb63bde82 (Unpacked)

Nume PPD CRU U/DUC. Windows Description El wohotsze 22 13.44 JUCAL SENCE Windows 91-ZUDARZ, El wohotsze 132 22.21 13.44 JUCAL SENCE Windows 91-ZUDARZ, El wohotsze 132 22.21 JUCAL SENCE Windows 91-ZUDARZ, Introductare 138 1.38 Mis JUCAL SENCE Windows 91-ZUDARZ, El wohotsze 132 2.22 Mis JUCAL SENCE Windows 91-ZUDARZ, Introductare 138 1.38 Mis JUCAL SENCE Windows 91-ZUDARZ, El wohotsze 130 JUCAL SENCE Windows 91-ZUDARZ, Introductare 138 Introductare 138 Introductare 139 JUCAL SENCE Windows 91-ZUDARZ, El wohotsze 130 JUCAL SENCE Kindows 91-ZUDARZ, Introductare 139 JUCAL SENCE Kindows 91-ZUDARZ, El wohotsze 130 JULA JULA SISTEN Winaws SCA Helper- Introductare, 1400 JUCAL SENCE Kindows 91-ZUDARZ, In wohotsze 130 JULA JULA SISTEN <td< th=""><th>ocesses Services Network Disk</th><th></th><th></th><th></th><th></th></td<>	ocesses Services Network Disk				
□ Fride 0 897 MB JUCAL SERVIC Windows TP-200R.Z. □ Fride 22 134.4	ame	PID CPU I/O tot	Private User name Description		
Image: Status 22 13.44 JLOCAL SERVICE Windows D+ 22.000.1. Image: Status 64 85.1 12.22 11.44 JLOCAL SERVICE Windows D+ 22.000.1. Image: Status 13.2 2.2 2.2 11.44 JLOCAL SERVICE Windows D+ 22.000.1. Image: Status 13.8 13.8 13.8 13.8 13.8 13.8 14.8 14.1 Status 14.4 JLLUSSTEM Windows D+ 22.000.1. Image: Status 14.6 14.1 MLLUSSTEM Windows D+ 22.000.1. Image: Status 14.6 MLLUSSTEM Windows D+ 22.000.1. Image: Windows 12.2 2.7.1 Mindows D+ 22.000.1. Image: Status 14.6 MLLUSSTEM Windows D+ 22.000.1. Image: Windows 12.2 17.1 Mindows D+ 22.000.1. Image: Windows D+ 22.000.1. Image:	svchost.exe	80	8.97 MB¥LOCAL SERVICE Windows サービスのホス		
If wrindtate 664 88 bp 12.22 NTAULXYSTEM Windows 7: CX0RTA. If wrindtate 132 2.22 MB JUCAL SERVICE Windows 7: CX0RTA. If wrindtate 133 2.22 MB JUCAL SERVICE Windows 7: CX0RTA. If wrindtate 133 2.22 MB JUCAL SERVICE Windows 7: CX0RTA. If wrindtate 138 JURAL XISSTEM Windows 7: CX0RTA. If wrindtate 1864 3.44 MB NTAULXYSTEM Windows 7: CX0RTA. If wrindtate 1864 12.24 MB TAULXYSTEM Windows 7: CX0RTA. If wrindtate 282 6.64 MB NTAULXYSTEM Winwes Yook Alleger. If wrindtate. 282 2.65 MB NTAULXYSTEM Winwes Yook Alleger. If wrindtate. 282 2.64 MB JULXYSTEM Winwes Yook Alleger. If wrindtate. 232 12.94 MB NTAULXYSTEM Windows 7: CX0RTA. If wrindtate. 552 2.46 MB JULXYSTEM Windows 7: CX0RTA. If wrindtate. 554 13.34 MB TAULXYSTEM Windows 7: CX0RTA. If wrindtate. 554 13.	📧 svchost.exe	272	13.44¥LOCAL SERVICE Windows サービスのホス		– U X
Image: Seventation of the state of the	svchost.exe	684 88 B/s	12.52 NT AUT¥SYSTEM Windows サービスのホス	27-1ル ホーム 共有 表示	~
If solvidate 132 2.22 MB JUCAL SERVICE Windows 19-ZADRA, If solvidate 138 1.84 MB JUCAL SERVICE Windows 19-ZADRA, If solvidate 139 5.44 MB NTALL'SSYSTEM JZ7-7 TZVZADZ, ZZZAD, If solvidate 1902 0.56 677 MB NTALL'SSYSTEM JZ7-7 TZVZADZ, If windows 1900 0.56 677 MB NTALL'SSYSTEM VANore 50x Core Se. If windows 12, 22 MB 1.44 MB NTALL'SSYSTEM VANore 50x Core Se. If windows 12, 22 MB 1.44 MB NTALL'SSYSTEM VANore 50x Core Se. If windows 12, 22 MB 1.44 MB NTALL'SSYSTEM VANore 50x Core Se. If windows 12, 22 MB 1.44 MB NTALL'SSYSTEM VANore 50x Core Se. If windows 12, 22 MB 1.44 MB Norobit Se. 1.64 MB Korooh TMAND SP-2ZADRA, If windows 12, 22 MB 1.14 MB .10CAL SERVICE Windows 5-2. 1.64 MB Korooh TMAL'SSYSTEM Vindows 5-2. If windows 12, 23 MB DSKOL Window 5-2. 1.53 MB NTALL'SSYSTEM Windows 5-2. 1.53 MB NTALL'SSYSTEM Windows 5-2. If windows 12, 23 MB DSKOL Window 5-2. 1.53 MB NTALL'SSYSTEM Windows 5-2.	svchost.exe	1160	6.36 MB¥NETWORK SER\ Windows サービスのホス	e 🖂 🔶 - 🛧 📙 > ursnif	✓ ひ ursnifの検索
If Synchrotzee 138 1.81 MS VCAL SERVICE Windows D+Z007AL. if synchrotzee 156 5.4M S Windows D+Z007AL. VCAL SERVICE Windows D+Z007AL. If synchrotzee 158 5.6M S WINDOWS D+Z007AL. VCAL SERVICE VCAL SERVICE </td <td>svchost.exe</td> <td>1332</td> <td>2.32 MB¥LOCAL SERVICE Windows サービスのホス</td> <td></td> <td></td>	svchost.exe	1332	2.32 MB¥LOCAL SERVICE Windows サービスのホス		
mis poolsvoze 1908 S.4 MB NI AULXSYSTEM 27-7 mis scholtszee 1902 6.26 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 1902 6.26 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 1909 5.4 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 1909 5.4 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 1909 5.4 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 1902 2.55 MB NI AULXSYSTEM Window 17-12/00.7.2. mis wicholtszee 122 1.74 MB - AUCCA SERVICE Window 17-12/00.7.2. mis wicholtszee 122 1.74 MB - AUCCA SERVICE Window 17-12/00.7.2. mis wicholtszee 122 1.74 MB - AUCCA SERVICE Window 17-12/00.7.2. mis wicholtszee 124 6.43 MB DESKIO-JWINIO Window 17-12/00.7.2. mis wicholtszee 124 4.63 MB NI AULXSYSTEM Vindow 17-12/00.7.2. mis wicholtszee 124 0.09 216 NB NI AULXSYSTEM Vindow 17-12/07.7.9 mis wicholtszee 124 0.07 GesK BW NI AULXSYSTEM Vindow 17-20/07.7.9 -7-2.9.2. mis wicholtszee 124 0.07 GesK BW NI AULXSYSTEM Vindow 17-20/07.7.9 -7-2.9.2. mis wicholtszee 124	svchost.exe	1388	1.88 MB¥LOCAL SERVICE Windows サービスのホス	★ 01ッ0 70セス	
If sorkbattee 1964 9.19 M8 NT AULTSYSTEM Windows 923/08.2. If sorkbattee 1990 0.05 6.67 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 1900 1.54 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 2084 1.52 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 2084 1.52 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 2084 1.52 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 2024 2.62 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If motokideze 2322 2.77 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If synchosizes 322 1.74 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If synchosizes 322 1.59 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If synchosizes 322 2.37 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If windowses 564 4.54 M8 NT AULTSYSTEM Windows 9-2-23/08.2. If windowses 564 3.55 M8 NT AULTSYSTEM Windows 9-2-23/08.2.	🖶 spoolsv.exe	1508	5.4 MB NT AUT¥SYSTEM スプーラー サブシステム アプ	■ F201-y7 * uranifere	
Image: Section Sectin Section Section Sectin Section Section Section Section Section Se	svchost.exe	1864	9.19 MB NT AUT¥SYSTEM Windows サービスのホス	↓ ダウンロード ★	
□ mutoold.dee 190 0.05 6.67 /M NI AULTXYSTEM Vilware Tools Core Se. □ VURAditSvirka. 204 1.52 /M NI AULTXYSTEM Vilware Sock Alelper □ VURAditSvirka. 204 1.52 /M NI AULTXYSTEM Vilware Sock Alelper □ VURAditSvirka. 204 2.65 /M NI AULTXYSTEM Vilware Sock Alelper □ VURAditSvirka. 204 2.65 /M NI AULTXYSTEM Vilware Sock Alelper □ VURAditSvirka. 232 3.77 M NI AULTXYSTEM Vilware Sock Alelper □ Sochotece 512 1.47 MM NI AULTXYSTEM Vilkoooff %Rit>77 /L □ Sochotece 132 6.63 /M NI AULTXYSTEM Vindoovs 5e. □ Sochotece 132 1.15 /M NI AULTXYSTEM Vindoovs 5e. □ Sochotece 132 1.15 /M NI AULTXYSTEM Vindoovs 7eZokata □ Sochotece 132 1.91 /M NI AULTXYSTEM Vindoovs 7eZokata □ Sochotece 322 1.91 /M NI AULTXYSTEM Vindoovs 7eZokata □ Sochotece 322 2.26 /M 1.91 /M NI AULTXYSTEM Vind	svchost.exe	1892	6.26 MB NT AUT¥SYSTEM Windows サービスのホス	B F41X2F #	
Trum 3device.zee 1908 1.4 M8 NT AULXYSTEM ViMware SVGA Helper Trum 3device.zee 1920 2.65 M8 NT AULXYSTEM Vimware Guest Authen Trum 3device.zee 2372 3.77 M8 NT AULXYSTEM Vimware Guest Authen Trum 3device.zee 2372 3.77 M8 NT AULXYSTEM Vimware Guest Authen Trum 3device.zee 252 2.46 M8 NT AULXYSTEM Vimoso 17 %R Y27 J Trum 3device.zee 152 1.74 M8 -VICAL SERVICE Windows 5 – ZX0 RX Searchindevice 364 Trum 3device.zee 352 1.53 M8 NT AULXYSTEM Windows 7 – ZX0 RX Searchindevice 364 Trum 3device.zee 6560 1.53 M8 NT AULXYSTEM Windows 7 – ZX0 RX -Z -Z -Z Trum 3device.zee 562 1.53 M8 NT AULXYSTEM Windows 10/20 / 70/21/7 74 -Z <	🚾 vmtoolsd.exe	1900 0.05	6.67 MB NT AUT¥SYSTEM VMware Tools Core Se	E 2074 *	
□ Windowrvice 2084 1.52 MB NIX AUT.XSYSTEM VAware SVGA Helper □ Workinskiewice 209 2.55 MB NIX AUT.XSYSTEM VAware SUGA Helper □ dilhostexe 2372 3.77 MB NIX AUT.XSYSTEM VAware SugA Helper □ winking 2.12 1.74 MB XVLCXSYSTEM VAware SUGA NIX AUT.XSYSTEM VAware SUGA NIX AUT.XSYSTEM □ winking 1.36 6.43 MB 2.80.5 NIX AUT.XSYSTEM Windows 5P-2.20.87.2. □ winking 1.33 MB NIX AUT.XSYSTEM Windows 5P-2.20.87.2. □ □ □ sychostexe 362 1.53 MB NIX AUT.XSYSTEM Windows 5P-2.20.87.2. □ □ □ sychostexe 664 4.63 MB DIX AUT.XSYSTEM Windows 5P-2.20.87.2. □ □ □ □ system 1.33 MB NIX AUT.XSYSTEM Windows 5P-2.20.87.2. □	✓ III vm3dservice.exe	1908	1.4 MB NT AUT¥SYSTEM VMware SVGA Helper	iles	
III VGAuh/Service. 1920 265 M8 NTAULXSYSTEM Winver Guest Authen. III Ministerice. 247 377 M8 NTAULXSYSTEM Kourogate III Suchostee 252 2.66 M8 Ministerice. 348 2002 Nonsoft Vindows 9-230x7. III sychostee 1364 6.43 M8 DESKTO_XWinit0 Windows 9-230x7. IIII Suchostee IIII Suchostee 1364 6.43 M8 DESKTO_XWinit0 Windows 9-230x7. III sychostee 6.62 1.53 M8 NTAULXSYSTEM Windows 9-230x7. IIIII Suchostee IIIII Suchostee IIIII Suchostee IIIII Suchostee IIIII Suchostee IIIII Suchostee IIIIII Suchostee IIIII Suchostee IIIII Suchostee IIIII Suchostee IIIIIIIII Suchostee IIIIIIIII Suchostee IIIIIIIIIII Suchostee IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	💽 vm3dservice	2084	1.52 MB NT AUT¥SYSTEM VMware SVGA Helper	Noriben-master	
■ Idihosteve 2372 3.77 MB NT AUT_XYSTEM CON Surrogate Smsdtcave 252 2.46 MB XHENDORS KER Microsoft XMIRDYT S vrbostove 512 1.74 MB VLOCAL SERVICE Windows 9+220/kT.A. S vrbostove 1344 6.43 MD DESKTO_XWINID Windows 9+220/kT.A. S vrbostove 1354 6.51 MB NT AUT_XSYSTEM Kindows 9+220/kT.A. S vrbostove 1354 6.51 MB NT AUT_XSYSTEM Kindows 9+220/kT.A. S vrbostove 1364 6.51 MB NT AUT_XSYSTEM Kindows 9+220/kT.A. S vrbostove 1364 6.51 MB NT AUT_XSYSTEM Kindows 9+270/kT.A. S vrbostove 1364 6.51 MB NT AUT_XSYSTEM Kindows 9+270/kT.A. S windognove 560 1.51 MB NT AUT_XSYSTEM Kindows 9+270/kT.A. S windostove 128 MB 0.51 MB NT AUT_XSYSTEM Kindows 9+270/kT.A. S windostove 128 MB 0.51 MB NT AUT_XSYSTEM Kindows 9+270/kT.A. M Maccula 0.10 1113.8. <td< td=""><td>VGAuthService</td><td>1920</td><td>2.65 MB NT AUT¥SYSTEM VMware Guest Authen</td><td>plugins</td><td></td></td<>	VGAuthService	1920	2.65 MB NT AUT¥SYSTEM VMware Guest Authen	plugins	
Msdtczee 2652 2.46 MB _VNCTWORK SERN Microsoft Vindows 5/27 Swichostzee 512 1.74 MB _VNCost SERV(2: Windows 5-2,20,37.2, Swichostzee 364 6.43 MB DESKT0_Win10 Windows 5-2,20,37.2, Swichostzee 365 1.53 MB NT AUL XSYSTEM Windows 5-2,20,37.2, Swichostzee 365 1.53 MB NT AUL XSYSTEM Windows 5-2,20,37.2, Swichostzee 452 3.65 MB NT AUL XSYSTEM Windows 5-2,20,37.2, Swichostzee 454 4.67 MB NT AUL XSYSTEM Windows 5-2,20,37.2, Swichostzee 564 1.53 MB NT AUL XSYSTEM Vindows 5-2,20,37.2, Swichostzee 564 3.65 MB NT AUL XSYSTEM Vindows 5-2,20,37.2, Swichostzee 564 3.65 MB NT AUL XSYSTEM Vindows 5-2,20,37.2, Swichostzee 564 3.65 MB NT AUL XSYSTEM Vindows 5-2,20,37.2, Swichostzee 564 3.65 MB NT AUL XSYSTEM Vindows 5-2,20,37.2, Swichostzee 564 3.65 MB NT AUL XSYSTEM Vindows 52,77.7 Vin/10	dllhost.exe	2372	3.77 MB NT AUT¥SYSTEM COM Surrogate	plugins	
Image: Synchosteve Siz 17.4 MB+UCAL SERVICE Windows 9-42/00.7.2. Image: Searchindexene	som and the second seco	2652	2.46 MB¥NETWORK SER\ Microsoft 分散トランザ	OneDrive	
Searchindexer. 348 280.5. NT AUT. SYSTEM Microsoft Windows 5e. III sychostexe 1364 643 MB DESKTOWinito Windows 5H-2X0.8t.2. III sychostexe 650 153 MB NT AUT. SYSTEM Windows 5H-2X0.8t.2. III sychostexe 662 153 MB NT AUT. SYSTEM Windows 5H-2X0.8t.2. III sass.exe 624 467 MB NT AUT. SYSTEM Vindows 1D/2X9.7T.2. III diagon.exe 564 302 0.07. DESKTOWiniti UZ777-7-7-7. III diagon.exe 164 0.07 DESKTOWiniti UZ777-7-7-7. III wrobisd.exe 124 0.07 DESKTOWiniti UXmare Tools Core Se III wrobisd.exe 124 0.07 DESKTOWiniti Microsoft Core Se III wrobisd.exe 126 0.46 17.59. DESKTOWiniti Microsoft Core Se IIII wrobisd.exe 124 0.07 B8 MB DESKTOWiniti Microsoft Core Se IIII wrobisd.exe 124 0.07 B8 MB DESKTOWiniti Microsoft Core Se IIIII wrobisd.exe 128 0.46 17.59.	svchost.exe	512	1.74 MB¥LOCAL SERVICE Windows サービスのホス		
● Sychostexe 1364 6.43 MB DESKTO_XWIN10 Windows サービスのホス	SearchIndexer.e	348	28.05 NT AUT¥SYSTEM Microsoft Windows Se		
I Sychostexe 3032 159 MB NT AUT_XSYSTEM Windows 9-200RA. I Sychostexe 650 1.53 MB NT AUT_XSYSTEM Windows 9-200RA. I Sassexe 624 467 MB NT AUT_XSYSTEM Vindows 9-200RA. I Sassexe 624 467 MB NT AUT_XSYSTEM Vindows 9-200RA. I Sassexe 624 467 MB NT AUT_XSYSTEM Vindows 9-270RA. I Sassexe 624 467 MB NT AUT_XSYSTEM Vindows 0747 77). I windows 50 7777 h 7-177. I windows 50 7777 h 777. I windows 50 564	svchost.exe	1364	6.43 MB DESKTO¥Win10 Windows サービスのホス	→ ネットワーク	
If synchostexe 6560 1.53 MB NT AUT_XSYSTEM Windows 5/2007.2 IF Issassexe 624 4.67 MB NT AUT_XSYSTEM Local Security Authorit IF Issassexe 624 4.67 MB NT AUT_XSYSTEM Local Security Authorit IF Grissexe 624 3.65 MB NT AUT_XSYSTEM Vindows D7772.h f-1/(-7)-79.9 IF windogon.exe 564 3.65 MB NT AUT_XSYSTEM Windows D73777.h f-1/(-7)-79.9 IF windogon.exe 884 0.10 111.38. Windows D7377.7 f-1/(-7)-79.7 IF windogon.exe 884 0.10 111.38. Windows D7377.7 f-1/(-7)-79.7 IF windogon.exe 329 0.32 302.07 DESKTO¥Win10 197.07.9 IF windogon.exe 128 0.07 684 B/s 20.14 DESKTO¥Win10 Windows Defender no IF windogon.exe 6288 16.94 DESKTO¥Win10 Windows Defender no IF windogon.exe 7016 3.89 MB DESKTO¥Win10 Windows Defender no If windogon.exe 7016 3.89 MB DESKTO¥Win10 Windows Defender no	📧 svchost.exe	3032	1.59 MB NT AUT¥SYSTEM Windows サービスのホス		
El sass.exe 624 4.67 MB NT AUT.#SYSTEM Local Security Authorit Er srss.exe 492 0.09 216 B/s 191 MB NT AUT.#SYSTEM 075/72/-17-02/ Winlogon.exe 564 3.65 MB NT AUT.#SYSTEM Windows 07/72/-77/ Image: 275% Physical memory: L28 GB (31.97%) Processes: 2 Vindows 07/72/-77 Image: 275% Physical memory: L28 GB (31.97%) Processes: 3 Vindows 07/72/77/72/-77 Vindows 07/72/77/72/-77 Image: 275% Physical memory: L28 GB (31.97%) Processes: 3 De SkTO#Win10 Windows Defender no	📧 svchost.exe	6560	1.53 MB NT AUT¥SYSTEM Windows サービスのホス		
 C STRS.EXE 492 0.09 216 B/s 1.91 MB NT AUT_XSYSTEM グライアントサーバーラック_ 3.65 MB NT AUT_XSYSTEM Window.BYAY アブリ C dwm.exe 848 0.10 111.38. Window.JDWM-1 TZ/JP-ブ- MSASCuiL.exe 1680 2.81 MB DESKTO¥Win10 Undows Defender no Wintoolsd.exe 16.94. DESKTO¥Win10 Windows Of AP JT - F OneDrive.exe 6288 16.94. DESKTO¥Win10 Windows Defender no Processes Sakura.exe 7016 3.89 MB DESKTO¥Win10 Processes UUtage 2.75% Physical memory: 1.28 G8 (31.97%) Processes: 2 	Isass.exe	624	4.67 MB NT AUT ¥SYSTEM Local Security Authorit		
* Winlogon.exe 564 3.65 MB NT AUT_XSYSTEM Windows ログオン アブリ * dwm.exe 884 0.10 111.38. Windows ログオン アブリ * explorer.exe 3292 0.32 302.07 DESKTO¥Win10 17.70-7- * MSASCuiL.exe 1680 2.81 MB DESKTO¥Win10 Windows Defender no Windows Defender no * OneDrive.exe 6288 1.6.94 DESKTO¥Win10 Wincrosoft OneDrive. * ProcessHacker.exe 1468 0.46 17.59 DESKTO¥Win10 Process Hacker * Sakura.exe 7016 3.89 MB DESKTO¥Win10 t// yoot Yoot VUUsage: 2.77% Physical memory: 1.28 GB (31.97%) Processes: 52 Yoot	CSrss.exe	492 0.09 216 B/s	1.91 MB NT AUT¥SYSTEM クライアント サーバー ランタ		
 ■ dwm.exe ■ 884 0.10 111.38. Windo¥DWM-1 デスクトップ ウィンドウマネ ■ explorer.exe 3292 0.32 302.07. DESKTO¥Win10 I/D Z/D - ラ- ① MSASCuiL.exe 1680 2.81 MB DESKTO¥Win10 Windows Defender no Wintoolsd.exe 124 0.07 684 B/s 20.14 DESKTO¥Win10 Windows Defender no Wintoolsd.exe 124 0.07 684 B/s 20.14 DESKTO¥Win10 Wincosoft OneDrive ProcessHacker.exe 1468 16.9 0.46 17.59 DESKTO¥Win10 ProcessHacker.exe 1468 0.46 17.59 DESKTO¥Win10 ProcessHacker.exe 1807目 Tubuget 2.75% Physical memory: 1.28 GB (31.97%) Processes 52 	🖭 winlogon.exe	564	3.65 MB NT AUT¥SYSTEM Windows ログオン アプリ		
mexplorer.exe 3292 0.32 302.07 DESKTO¥Win10 I/Dスプローラー WMSASCuiL.exe 1680 2.81 MB DESKTO¥Win10 Windows Defender no Wmtoolsd.exe 124 0.07 684 B/s 20.14<	📧 dwm.exe	884 0.10	111.38 Windo¥DWM-1 デスクトップ ウィンドウ マネ		
If MSASCuiL.exe 1680 2.81 MB DESKTO¥Win10 Windows Defender no Image: 124 0.07 684 B/s 20.14 DESKTO¥Win10 VMware Tools Core Se Image: 275% Physical memory: 1.28 GB (31.97%) Processer 52	explorer.exe	3292 0.32	302.07 DESKTO¥Win10 エクスプローラー		
□ vmtoolsd.exe 124 0.07 684 B/s 20.14 DESKTO¥Win10 VMware Tools Core Se ● OneDrive.exe 6288 16.94 DESKTO¥Win10 Microsoft OneDrive ● ProcesssHacker.exe 1468 0.46 17.59 DESKTO¥Win10 Process Hacker ③ sakura.exe 7016 3.89 MB DESKTO¥Win10 サクラエディタ	MSASCuiL.exe	1680	2.81 MB DESKTO¥Win10 Windows Defender no		
OneDrive.exe 6288 16.94 DESKTO¥Win10 Microsoft OneDrive ProcessHacker.exe 1468 0.46 17.59 DESKTO¥Win10 Process Hacker 3 sakura.exe 7016 3.89 MB DESKTO¥Win10 サクラエディタ Vulage: 2.75% Physical memory: 1.28 GB (31.97%) Processes: 52 Processes: 52	🔤 vmtoolsd.exe	124 0.07 684 B/s	20.14 DESKTO¥Win10 VMware Tools Core Se	1 俄の項目	Bee a
ProcessHacker.exe 1468 0.46 17.59 DESKTO¥Win10 Process Hacker ** sakura.exe 7016 3.89 MB DESKTO¥Win10 サクラエディタ Ucage: 2.75% Physical memory: 1.28 GB (31.97%) Processe: 52 ************************************	🗢 OneDrive.exe	6288	16.94 DESKTO¥Win10 Microsoft OneDrive		
Image: 7016 3.89 MB DESKTO¥Win10 サクラエディタ Ubsage: 2.75% Physical memory: 1.28 GB (31.97%) Processes: 52	ProcessHacker.exe	1468 0.46	17.59 DESKTO¥Win10 Process Hacker		
	🖺 sakura.exe	7016	3.89 MB DESKTO¥Win10 サクラエディタ		
	Illeaner 2 75% Dhusical memorer 1	28 (58 (31 97%) Processes 53	,		
	And the second sec	ne estanoine riocesses y			

mon - ショート カット



File Edit Jump Search View Debugger Lumina Options Windows Help



Future Work

Plugin being developed for Ghidra version



Updated Version 1.1 Released

https://github.com/LAC-Japan/IDA Plugin AntiDebugSeeker



README
 BSD-3-Clause license

IDA_Plugin_AntiDebugSeeker

Concept

This tool was created to assist those who are new to malware analysis or are not yet familiar with anti-debugging techniques. Through this tool, users can automatically extract potential anti-debugging methods used by malware, making it easier for analysts to take appropriate action.

Introduction

The main functionalities of this plugin are as follows:

- Extraction of Windows API that are potentially being used for anti-debugging by the malware (All subsequent API represent the Windows API)
- In addition to API, 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.



ß

:=

