

雲端軟體分析器

以模擬器建構線上系統程式分析環境

專題生：謝居安

指導教授：謝續平

惡意程式分析現況

- 工具為數眾多且各有特點,環境建置不易
- 分析工具易被惡意程式識別

與現有線上分析平台的不同

- ThreatExpert, VirusTotal, Anubis, CWSandbox
 - 提供自動化的分析報告
- 除了提供自動化分析外,此系統還提供
 - 可視可操作的VM環境
 - 直接在Web上進行Debugging
 - 先進的輔佐分析技術
 - Taint Analysis
 - Anti-anti-VM

系統功能簡介

- 檢視、修改虛擬機器的記憶體和硬碟內容
- 觀察虛擬機器網路封包
- 對程式進行單步執行，觀察暫存器、虛擬記憶體內容
- 對檔案、記憶體內容進行標記
- 將虛擬機器之被標記之硬碟磁區反轉為檔案或win registry

Debugging process in VM

The screenshot displays a Windows XP desktop environment within a virtual machine. The desktop includes icons for 'Resource Recycle Bin', 'nscp.exe', 'sslt_get.exe', 'sync.exe', 'winReg.exe', 'kmEnumPro', and 'QEMU_agent Xe'. A taskbar at the bottom shows several running processes, including 'QEMU_agent Xe' and 'krnEnumProc.exe'.

The main window is titled 'Process View - notepad.exe, PID : 1488'. It features several panes:

- Process list:** A table listing system processes. The 'services.exe' process (PID 524, CR3 050b9000) is highlighted as the debug target.
- Instruction View:** A table showing the current instruction stream for the target process.
- Memory View:** A table showing the memory contents at the current instruction address (0x0100739d).
- CPU View:** A list of CPU registers and their values.
- Breakpoint View:** A list of active breakpoints, with one at address 0x010073ac.

Process list:

pid	CR3	name
4	00039000	System
304	02e2f000	smss.exe
404	03ee4000	csrss.exe
432	046aa000	winlogon.exe
524	050b9000	services.exe
536	05197000	lsass.exe
700	05bbc000	svchost.exe
768	06219000	svchost.exe
852	06862000	svchost.exe
1012	0803d000	svchost.exe
1044	08845000	svchost.exe
1112	08beb000	spoolsv.exe
1640	097be000	explorer.exe
2024	0c163000	ctfmon.exe
364	0d2ba000	alg.exe
396	0d748000	wscntfy.exe
1160	0eec0000	conime.exe
1364	007f8000	QEMU_agent.exe QEMU_agent.exe
1436	04e88000	cmd.exe cmd.exe
1456	05cb4000	krnEnumProc.exe krnEnumProc.exe

Instruction View:

Address	OP-code	Disassembled	Other
0100739d	6a70	push 0x70	
0100739f	6898180001	push 0x1001898	
010073a4	e8bf010000	call 0x1007568	
010073a9	33db	xor ebx,ebx	
010073ab	53	push ebx	
010073ac	8b3dcc100001	mov edi,ds:0x10010cc	
010073b2	ffd7	call edi	
010073b4	6681384d5a	cmp DWORD PTR [eax],0x5a4d	
010073b9	751f	jne 0x10073da	
010073bb	8b483c	mov ecx,DWORD PTR [eax+60]	
010073be	03c8	add ecx,eax	
010073c0	813950450000	cmp DWORD PTR [ecx],0x4550	

Memory View:

Address	Hex	Ascii
01007390	cc cc ff 25 bc 12 00 01 cc cc cc cc cc 6a 70 68	. . . % .
010073a0	98 18 00 01 e8 bf 01 00 00 33 db 53 8b 3d cc 10
010073b0	00 01 ff d7 66 81 38 4d 5a 75 1f 8b 48 3c 03 c8 f
010073c0	81 39 50 45 00 00 75 12 0f b7 41 18 3d 0b 01 00	. 9 p e .
010073d0	00 74 1f 3d 0b 02 00 00 74 05 89 5d e4 eb 27 83	. t . = .

CPU View:

EAX 00000000
ECX 0007FFB0
EDX 7C92E4F4
EBX 00000000
ESP 0007FFC4
EBP 0007FFF0
ESI 01CC8316
EDI EB927900
EIP 0100739D
D: 0 O: 0 S: 0 Z: 1 A: 0 P: 1 C: 0

Breakpoint View:

addr	type	active
0x010073ac	INS	<input checked="" type="checkbox"/>

File tainting and disk-sectors <--> files mapping

The screenshot displays a software interface for file tainting analysis. The main window has tabs for Monitor, Disk, Network, Physical Memory, and Taint Analysis. The 'Disk' tab is active, showing a search bar with 'goto' and a 'File Sectors' panel. The 'File Sectors' panel shows the File Path: /windows/system32/config/software, Offset: 0, and Sector number: 0x11ccdf ~ 0x1214de.

Below the search bar is a grid of sectors. The grid has columns for Address and Sectors. The addresses range from 0011ccd0 to 0011cd70. The sectors are colored green, red, or blue. The sectors from 0011ccd0 to 0011ccf0 are green. The sectors from 0011cd00 to 0011cd70 are red. The sectors from 0011cd10 to 0011cd20 are blue.

Below the grid is a section titled 'Belong to files:' with a 'Path' field containing /WINDOWS/system32/config/software.

Overlaid on the interface is a hex editor window titled 'Hex editor 0x239a0e00 - 0x239a35ff'. The hex editor shows a table with columns for Address, Hex, and Ascii. The hex editor is displaying the contents of the file /windows/system32/config/software. The hex editor shows the following data:

Address	Hex	Ascii
239a0e00	68 62 69 6e 00 40 00 00 00 10	h b i n . @
239a0e0a	00 00 00 00 00 00 00 00 00 00
239a0e14	00 00 00 00 00 00 00 00 00 00
239a0e1e	00 00 98 ff ff ff 6e 6b 20 00 n k
239a0e28	e0 0a 86 3a 80 69 ca 01 00 00 i
239a0e32	00 00 18 3f 00 00 00 00 00 00 ?
239a0e3c	00 00 00 00 ff ff ff ff ff ff
239a0e46	ff ff 01 00 00 00 c0 3f 00 00 ?
239a0e50	10 02 00 00 ff ff ff ff 00 00
239a0e5a	00 00 00 00 00 00 00 00 00 00

The hex editor also has 'save' and 'cancel' buttons at the bottom.