FORENSIC ANALYSIS REPORT

WinVolAuto Professional Suite

1. CASE INFORMATION

Analysis Date:	2026-02-16 18:26:36
Target File:	vm_memory_ 2.elf
File Path:	D:/Games/v m_memory_2 .elf
File Size:	3055.91 MB
Analyst:	WinVolAuto Automated Agent

2. EXECUTIVE SUMMARY

Risk Level: Critical
Total Risk Score: 260/100
Risk Probability: 97%

Mapped MITRE ATT&CK; Techniques:

T1055, T1564

Top Suspicious Processes:

PID	Probability
1416	17%
2600	17%
3116	14%
2984	14%
2888	14%

3. MALWARE CAPABILITIES

Persistence

Mechanisms to survive reboot or maintain foothold.

Evidence:

- Kernel/user callbacks present
- Kernel/user callbacks present
- Kernel/user callbacks present
- Kernel/user callbacks present
- Kernel/user callbacks present

Stealth

Hidden processes or hierarchy anomalies to avoid detection.

Evidence:

- Hidden process detected PID 3116
- Hidden process detected PID 2984
- Hidden process detected PID 2888
- Hidden process detected PID 2900
- Hidden process detected PID 3068

Code Injection

Injected or hidden code in process memory.

Evidence:

- Injected code suspected in explorer.exe PID 1416
- Injected code suspected in SearchFilterHo PID 2600

Key Findings:

- Detected 2 potential code injection sites (Risk: +80)
- Detected 6 hidden processes (DKOM) (PIDs: 3116, 2984, 2888, 2900, 3068, 2288) (Risk: +180)

4. RISK ASSESSMENT METHODOLOGY

The risk score is calculated based on a heuristic analysis of memory artifacts. The system assigns weighted scores to specific anomalies found during the scan:

Anomaly Type	Description	Risk Weight
Code Injection	Executable memory pages not backed by disk (often shellcode)	40 pts
Suspicious Parent	Processes spawned by unexpected parents (e.g., Word spawning CMD)	35 pts
Hidden Processes	Processes present in memory scan but unlinked from OS list (DKOM)	30 pts
Masqueradi ng	Process names mimicking system binaries (e.g., svhost.exe)	30 pts
Encoded Command	Base64 or hidden commands detected in command line arguments	25 pts
Unsigned Drivers	Kernel modules lacking valid digital signatures (Rootkits)	25 pts
Suspicious Network	Connection s to high-risk ports or known bad IPs	20 pts
Suspicious Path	System processes running from Temp or AppData folders	15 pts

5. DETAILED FINDINGS

Plugin: windows.callbacks

Enumerates kernel-mode callback registrations; anomalies can indicate rootkit behavior.

Callback	Detail	Module	Symbol	Type
2192008936	None	ntoskrnl	EtwpTraceL oadImage	PspLoadIma geNotifyRo utine
2190102843	None	ntoskrnl	ViCreatePr ocessCallb ack	PspCreateP rocessNoti fyRoutine
2304141784	None	ksecdd	None	PspCreateP rocessNoti fyRoutine
2304187798	None	cng	None	PspCreateP rocessNoti fyRoutine
2307503827	None	tcpip	None	PspCreateP rocessNoti fyRoutine
2299518460	None	CI	None	PspCreateP rocessNoti fyRoutine
2463511001	None	peauth	None	PspCreateP rocessNoti fyRoutine
2304869984	None	ndis	None	KeBugCheck CallbackLi stHead
2304869984	None	ndis	None	KeBugCheck CallbackLi stHead
2304869984	None	ndis	None	KeBugCheck CallbackLi stHead
2193758614	None	hal	None	KeBugCheck CallbackLi stHead
2300507949	PEAUTH	Wdf01000	None	KeBugCheck ReasonCall backListHe ad
2444604686	mouhid	mouhid	None	KeBugCheck ReasonCall backListHe ad
2444511932	HidUsb	HIDCLASS	None	KeBugCheck ReasonCall backListHe ad
2444445790	HidUsb	hidusb	None	KeBugCheck ReasonCall backListHe ad
2300507949	monitor	Wdf01000	None	KeBugCheck ReasonCall backListHe ad
2444181950	CRASHDUMP	crashdmp	None	KeBugCheck ReasonCall backListHe ad
2443061722	USBHUB	usbhub	None	KeBugCheck ReasonCall backListHe ad
2443061637	USBHUB	usbhub	None	KeBugCheck ReasonCall backListHe ad
2300507949	umbus	Wdf01000	None	KeBugCheck ReasonCall backListHe ad
... (73 more rows) ...	... (73 more rows) ...	... (73 more rows) ...	... (73 more rows) ...	... (73 more rows) ...

Plugin: windows.info

Analysis plugin results.

Value	Variable	__children
0x8280e000	Kernel Base	[]
0x185000	DTB	[]
file:///C: /Users/Ace r/AppData/ Roaming/Py thon/Python314/site- packages/v olatility3 /symbols/w indows/ntkrnlmp.pdb/ 00625D7D36 754CBEBA45 33BA9A0F3FE2-2.json. xz	Symbols	[]
False	Is64Bit	[]
False	IsPAE	[]
0 WindowsInt el	layer_name	[]
1 Elf64Layer	memory_lay er	[]
2 FileLayer	base_layer	[]
0x8292fc28	KdDebugger DataBlock	[]
7601.17514 .x86fre.wi n7sp1_rtm. 10	NTBuildLab	[]
1	CSDVersion	[]
0x8292fc00	KdVersionB lock	[]
15.7601	Major/Mino r	[]
332	MachineTyp e	[]
6	KeNumberPr ocessors	[]
2026-02-13 08:30:24+0 0:00	SystemTime	[]
C:\Windows	NtSystemRo ot	[]
NtProductW inNt	NtProductT ype	[]
6	NtMajorVer sion	[]
1	NtMinorVer sion	[]
... (4 more rows) ...	... (4 more rows) ...	... (4 more rows) ...

Plugin: windows.malfind

Scans for hidden or injected code in user mode memory (VADs). It looks for memory pages that are executable but not backed by a file on disk, a common indicator of malware injection.

CommitCharge	Disasm	End VPN	File output	Hexdump
2	"b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64 b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54 b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44 b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34"	92610559	Disabled	b0 00 eb 70 b0 01 eb 6c b0 02 eb 68 b0 03 eb 64 b0 04 eb 60 b0 05 eb 5c b0 06 eb 58 b0 07 eb 54 b0 08 eb 50 b0 09 eb 4c b0 0a eb 48 b0 0b eb 44 b0 0c eb 40 b0 0d eb 3c b0 0e eb 38 b0 0f eb 34
1	"84 43 d5 ec b6 11 00 01 ee ff ee ff 00 00 00 00 a8 00 76 00 a8 00 76 00 00 00 76 00 00 00 76 00 40 00 00 00 88 05 76 00 00 00 7a 00 3f 00 00 00 01 00 00 00 00 00 00 00 f0 0f 76 00 f0 0f 76 00"	7995391	Disabled	84 43 d5 ec b6 11 00 01 ee ff ee ff 00 00 00 00 a8 00 76 00 a8 00 76 00 00 00 76 00 00 00 76 00 40 00 00 00 88 05 76 00 00 00 7a 00 3f 00 00 00 01 00 00 00 00 00 00 00 f0 0f 76 00 f0 0f 76 00

Plugin: windows.netscan

Scans for network artifacts (TCP/UDP endpoints, listeners). Critical for identifying Command & Control (C2) connections.

Created	ForeignAddr	ForeignPort	LocalAddr	LocalPort
None	23.50.14.4 3	443	None	49170
2026-02-13 T08:27:23+ 00:00	*	0	fe80::c56b :3ab0:8095 :ad0f	1900
2026-02-13 T08:27:23+ 00:00	*	0	127.0.0.1	55442
None	23.50.14.4 3	443	None	49171
None	2600:140f: 5:2085::35 6e	443	None	49166
None	0.0.0.0	0	0.0.0.0	49153
None	0.0.0.0	0	0.0.0.0	135
None	0.0.0.0	0	0.0.0.0	135
None	::	0	::	135
None	0.0.0.0	0	0.0.0.0	49152
None	0.0.0.0	0	0.0.0.0	49152
None	::	0	::	49152
None	0.0.0.0	0	0.0.0.0	49153
None	::	0	::	49153
None	0.0.0.0	0	0.0.0.0	49154

None	0.0.0.0	0	0.0.0.0	49156
None	0.0.0.0	0	0.0.0.0	445
None	::	0	::	445
2026-02-13 T08:27:23+ 00:00	*	0	127.0.0.1	1900
2026-02-13 T08:25:23+ 00:00	*	0	10.0.2.15	137
... (24 more rows) ...	... (24 more rows) ...	... (24 more rows) ...	... (24 more rows) ...	... (24 more rows) ...

Plugin: windows.pslist

Lists all processes running on the system. This plugin traverses the list of active process structures in the kernel memory. It is useful for identifying running applications and system services.

CreateTime	ExitTime	File output	Handles	ImageFileName
2026-02-13 T08:25:19+ 00:00	None	Disabled	439	System
2026-02-13 T08:25:19+ 00:00	None	Disabled	34	smss.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	322	csrss.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	81	wininit.ex e
2026-02-13 T08:25:21+ 00:00	None	Disabled	170	csrss.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	116	winlogon.e xe
2026-02-13 T08:25:21+ 00:00	None	Disabled	194	services.e xe
2026-02-13 T08:25:21+ 00:00	None	Disabled	536	lsass.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	141	lsm.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	362	svchost.ex e
2026-02-13 T08:25:21+ 00:00	None	Disabled	249	svchost.ex e
2026-02-13 T08:25:21+ 00:00	None	Disabled	441	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	300	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	958	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	127	audiodg.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	265	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	367	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	290	spoolsv.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	313	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	154	taskhost.e xe

... (9 more rows) ...	... (9 more rows) ...	... (9 more rows) ...	... (9 more rows) ...	... (9 more rows) ...

Plugin: windows.psscan

Scans physical memory for process objects (EPROCESS). Unlike pslist, this can detect 'hidden' processes that have been unlinked from the OS process list (DKOM attacks).

CreateTime	ExitTime	File output	Handles	ImageFileName
2026-02-13 T08:27:23+ 00:00	None	Disabled	148	svchost.ex e
2026-02-13 T08:28:30+ 00:00	None	Disabled	282	SearchProt ocol
2026-02-13 T08:28:30+ 00:00	None	Disabled	104	SearchFilt erHo
2026-02-13 T08:28:56+ 00:00	2026-02-13 T08:28:56+ 00:00	Disabled	None	rundll32.e xe
2026-02-13 T08:27:23+ 00:00	None	Disabled	151	sppsvc.exe
2026-02-13 T08:27:23+ 00:00	None	Disabled	316	svchost.ex e
2026-02-13 T08:28:56+ 00:00	2026-02-13 T08:28:56+ 00:00	Disabled	None	rundll32.e xe
2026-02-13 T08:25:21+ 00:00	None	Disabled	116	winlogon.e xe
2026-02-13 T08:25:21+ 00:00	None	Disabled	441	svchost.ex e
2026-02-13 T08:29:24+ 00:00	2026-02-13 T08:30:14+ 00:00	Disabled	None	notepad.ex e
2026-02-13 T08:25:21+ 00:00	None	Disabled	536	lsass.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	141	lsm.exe
2026-02-13 T08:25:21+ 00:00	None	Disabled	362	svchost.ex e
2026-02-13 T08:25:21+ 00:00	None	Disabled	249	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	300	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	958	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	127	audiodg.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	265	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	367	svchost.ex e
2026-02-13 T08:25:22+ 00:00	None	Disabled	290	spoolsv.ex e
... (15 more rows) ...	... (15 more rows) ...	... (15 more rows) ...	... (15 more rows) ...	... (15 more rows) ...

Plugin: windows.pstree

Displays processes in a tree structure, showing parent-child relationships. This helps identify suspicious spawning behavior (e.g., cmd.exe spawned by a web browser).

Audit	Cmd	CreateTime	ExitTime	Handles
None	None	2026-02-13 T08:25:19+ 00:00	None	439
\Device\Ha rddiskVolu me1\Window s\System32 \csrss.exe	%SystemRoo t%\system3 2\csrss.ex e ObjectDire ctory=\Win dows SharedSect ion=1024,1 2288,512 Windows=On SubSystemT ype=Window s ServerDll= basesrv,1 ServerDll= winsrv:Use rServerDll Initializa tion,3 ServerDll= winsrv:Con ServerDllI nitializat ion,2 ServerDll= sxssrv,4 ProfileCon trol=Off MaxRequest Threads=16	2026-02-13 T08:25:21+ 00:00	None	322
\Device\Ha rddiskVolu me1\Window s\System32 \wininit.e xe	wininit.ex e	2026-02-13 T08:25:21+ 00:00	None	81
\Device\Ha rddiskVolu me1\Window s\System32 \csrss.exe	%SystemRoo t%\system3 2\csrss.ex e ObjectDire ctory=\Win dows SharedSect ion=1024,1 2288,512 Windows=On SubSystemT ype=Window s ServerDll= basesrv,1 ServerDll= winsrv:Use rServerDll Initializa tion,3 ServerDll= winsrv:Con ServerDllI nitializat ion,2 ServerDll= sxssrv,4 ProfileCon trol=Off MaxRequest Threads=16	2026-02-13 T08:25:21+ 00:00	None	170
\Device\Ha rddiskVolu me1\Window s\System32 \winlogon. exe	winlogon.e xe	2026-02-13 T08:25:21+ 00:00	None	116
\Device\Ha rddiskVolu me1\Window s\explorer .exe	C:\Windows \Explorer. EXE	2026-02-13 T08:25:22+ 00:00	None	876