MIMOSA: Reducing Malware Analysis Overhead using Covering

Presenter: Mohsen Ahmadi

TDSC submission version - 2021

Nodes mapping: cost function metrics

Node	Backend	configuration	installation time	machine deploy time	cuckoo deploy time	pafish test
hopper1	KVM	qemu_patched_conf1	536.378853083s	3m0.784s	73.1922631264s	41.3594198227s
		qemu_patched_conf2	536.378853083s		69.9361619949s	45.833286047s
hopper2	VMWare	vmware_conf3	477.04450798s	1m7.059s	99.936568022s	27.6494090557s
hopper4		vmware_conf2	477.04450798s	10m44.653s	149.299293041s	27.5555241108s
hopper5		vmware_conf2_vmtools	477.04450798s	1m13.526s	161.119428158s	27.5111250877s
hopper6	KVM	qemu_legacy_conf1	538.147130966s	5m27.364s	100.959413052s	46.4497020245s
		qemu_legacy_conf2			105.494900942s	49.5711770058s
hopper8	Virtualbox	vbox_conf1_guestadditions	422.747698069s	2m21.955s	61.5865690708s	45.6178998947s
		vbox_conf2_guestadditions			62.7421720028s	25.1132590771s
hopper3		vbox_conf1	422.747698069s	1m13.356s	61.2738249302s	31.7570650578s
		vbox_conf2	304.682353973s		60.0014090538s	42.8423449993s
hopper7	QEMU	qemu_legacy_conf1	543.30523181s	5m27.364s	236.659236908s	122.378976107s
		qemu_legacy_conf2			213.200241089s	121.143641949s

*(13 configs for 4 HyperV backends)

Artifacts Mitigation: which artifacts we mitigate per each VM config

			Process		CPU								Disk				
Index	**Backend**	**configuration**	**Process Detection**	**debugger present**	**CPUID ***	**RDTSC**	**count # < 2**	**Invalid Instruction**	**GetTick Count**	**HCI**	**BIOS**	**File check Drivers**	**HDD / SCSI**	**Disk size < 60GB ****	**Memory < 1GB**	**MAC address ***	**ACPI DSDT**
1	**KVM**	qemu_patched_conf1	True	True	False	False	True	True	False	True	True	True	True	False	False	True	True
2		qemu_patched_conf2	True	True	False	False	True	True	False	True	True	True	True	False	True	False	True
3	**VMWare**	vmware_conf3	True	True	True	False	True	False	False	True	True	True	True	False	False	True	True
4		vmware_conf2	True	True	False	False	False	False	False	True	False	True	False	False	True	False	True
5		vmware_conf2_vmtools	False	True	False	False	True	False	False	True	False	False	False	False	True	False	True
6	**KVM***	qemu_legacy_conf1	True	True	False	False	True	True	False	True	**True**	True	False	False	True	True	True
7		qemu_legacy_conf2	True	True	False	False	False	True	False	True	**True**	True	False	False	False	False	True
8	*** Virtualbox**	vbox_conf1_guestadditions	False	True	False	False	False	True	False	True	***True***	False	True	True	False	False	False
9		vbox_conf2_guestadditions	False	True	False	False	True	True	False	True	False	False	True	True	False	True	True
10		vbox_conf1	True	True	True	False	True	True	False	True	True	True	True	True	True	False	False
11		vbox_conf2	True	True	False	False	False	True	False	True	False	True	True	True	False	True	False
12	**QEMU**	qemu_legacy_conf1	True	True	True	True	True	True	True	True	True	True	True	False	False	True	True
13		qemu_legacy_conf2	True	True	True	False	True	True	False	True	True	True	True	False	True	False	True

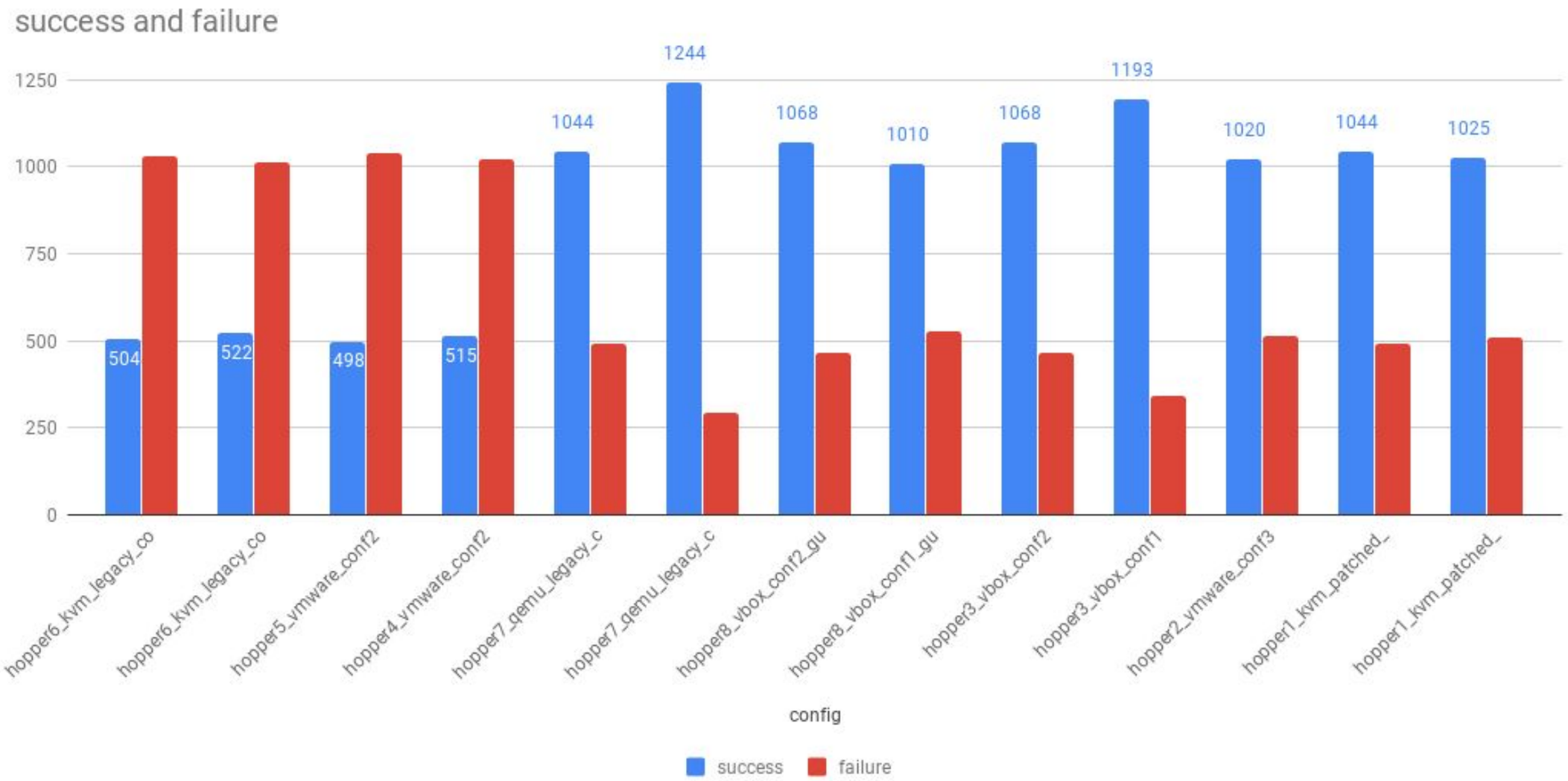
Note: we don't have introduced any protection against sandboxes, so the samples which are checking for sandbox registry artifacts will fail the whole protection we have per each config. It's under the following evasion category which I didn't set the bit here, but we should have it, if it's necessary.

"Detecting sandboxes by checking registry keys artifacts", "Ability to detect if Sleep() function is patched"

Faithful mapping: a mapping between the evasion techniques vs. mitigation techniques employed

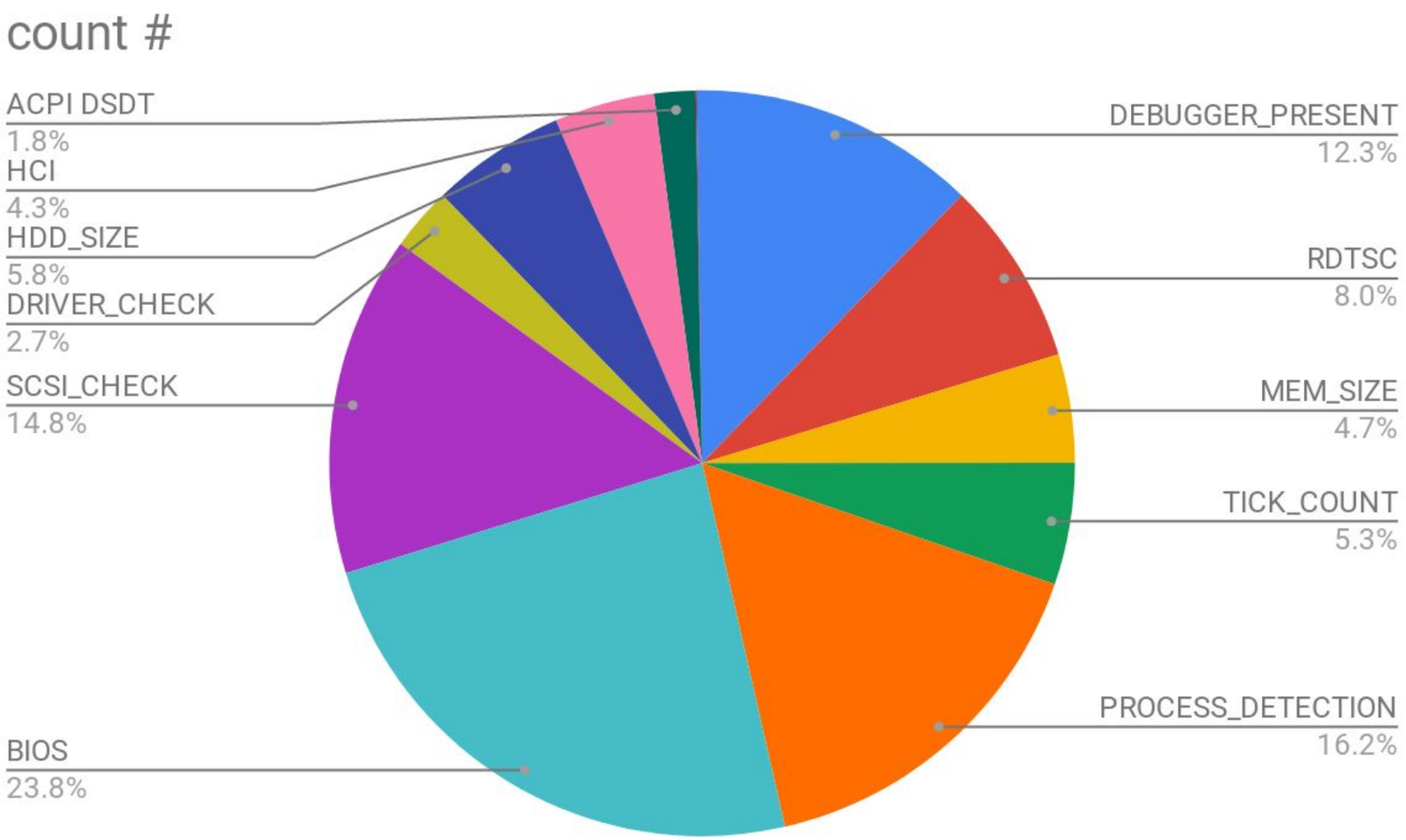
Index	Evasion Techniques	Mitigation
1	Ability to check the disk size, Potential detection of virtual environment (IOCTL_DISK_GET_LENGTH_INFO)	Disk size < 60GB
2	Ability to retrieve the current memory availability	Memory < 1GB
3	Trying to detect analysis virtual environment (BIOS detection), Trying to detect virtual environment by checking bios information from WMI	BIOS
4	Trying to detect analysis virtual environment (HDD detection)	HDD / SCSI
5	Trying to detect analysis virtual environment (drivers detection)	File Check Drivers
6	Ability to detect sandbox by checking mouse activity, Ability to retrieve a list of keyboard layouts	HCI
7	Timing Detection (rdtsc_GetTickCount)	GetTickCount
8	Potential Anti-VM time analysis check using rdtsc, Timing Detection (rdtsc_GetTickCount), Trying to detect analysis virtual environment (timing analysis detection)	RDTSC
9	Trying to detect analysis virtual environment (processor detection)	CPU # count
10	Detecting debugger by checking debug port, Detecting debugger by checking windows class name	IsDeubuggerPresent
11	Searching for specific processes: vmmouse.sys (analysis tool detection)	Process Detection
12	Switching processor mode from 32 to 64 bits (emulation escape)	Invalid Instruction
13	Detecting VirtualBox by enumerating ACPI registry keys	ACPI / DSDT
14	??	MAC
15		CPUID
16	Postponing the sample execution, Possibly stalling against analysis environment (sleep)	Sleep
17	Trying to detect analysis virtual environment (PnP device detection)	??
18	Trying to detect analysis virtual environment (window name detection), Trying to enumerate security products installed on the system from WMI, Trying to detect analysis virtual environment (computer name detection)	

Success vs. Failure



*) Total number of sample with evasion techniques employed are 1535.

Ratio: artifacts frequency per each category in the whole dataset



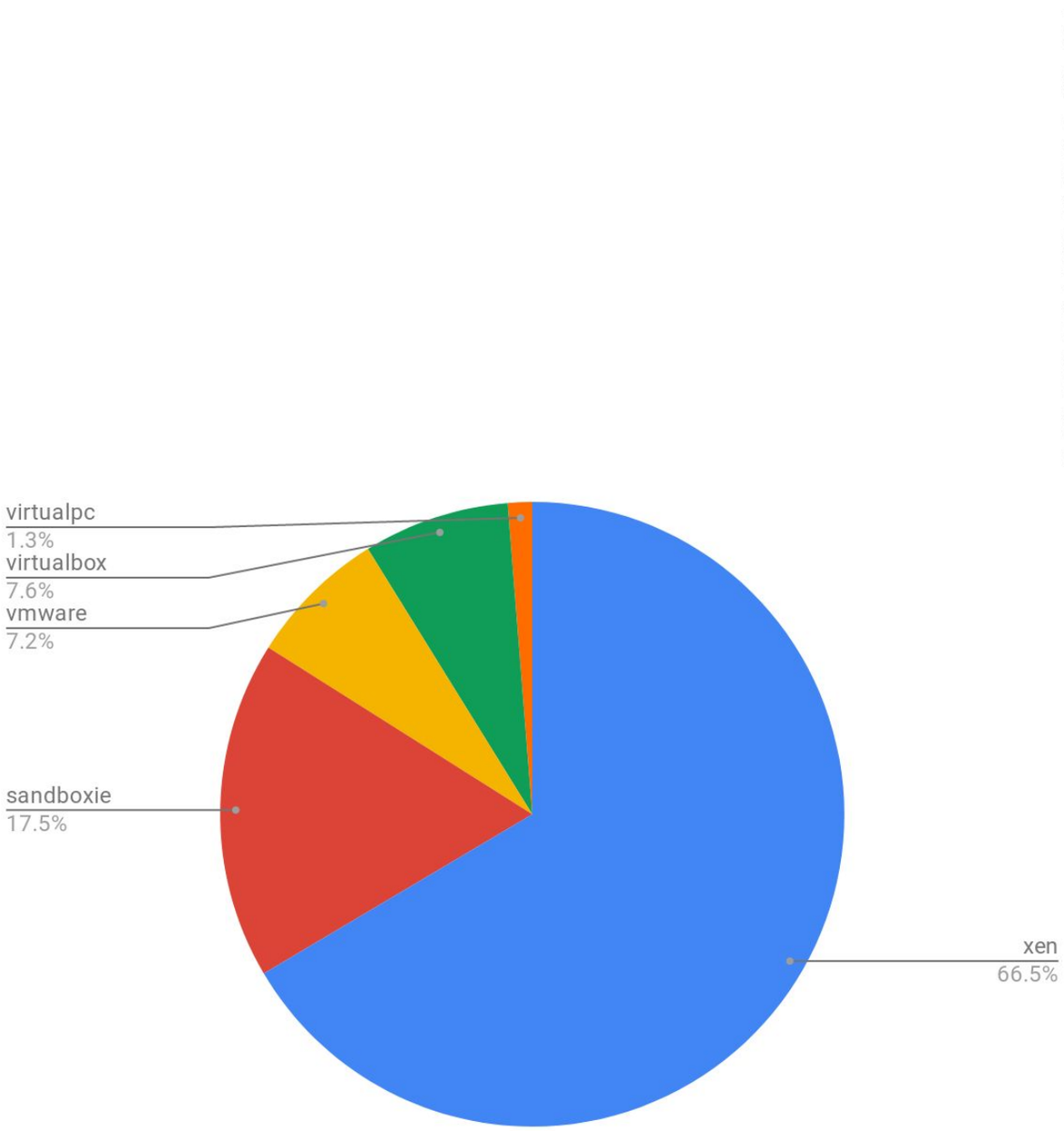
BIOS detection: different ways used by malware samples to detect BIOS remained artifacts

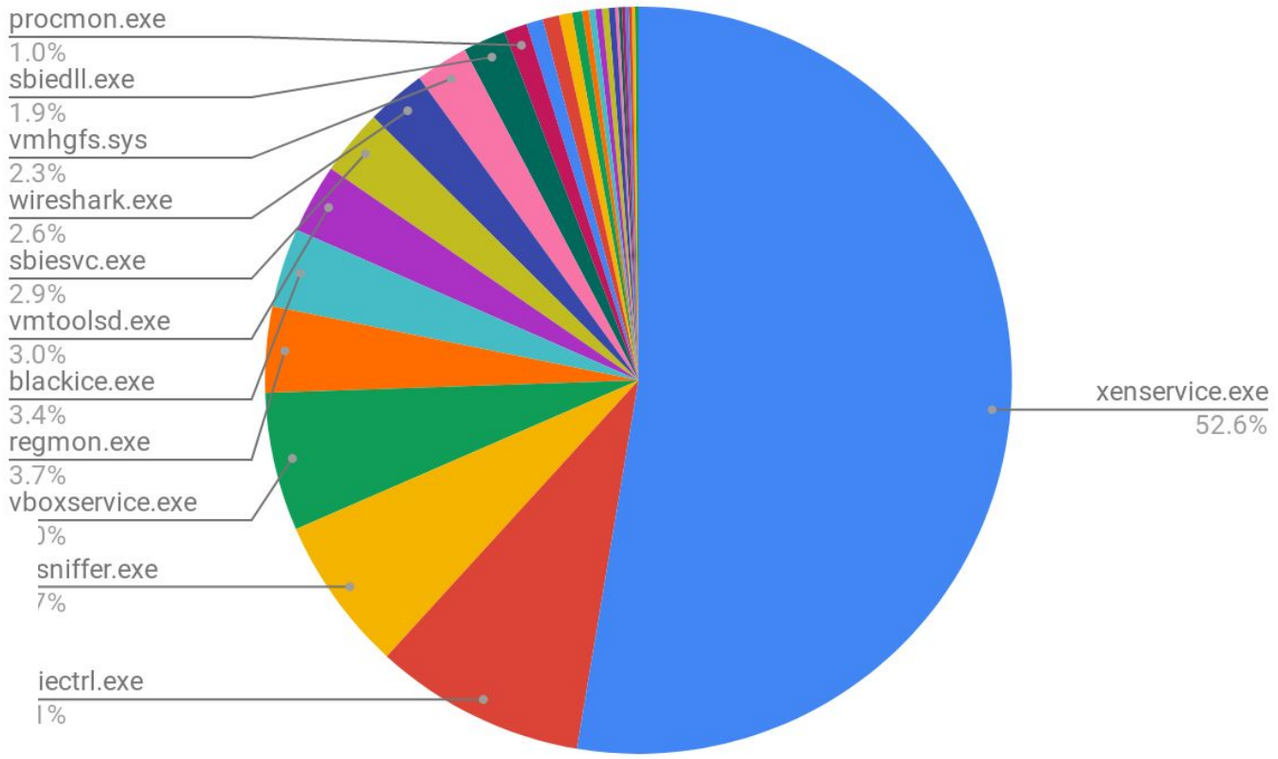
- WMIC
  - wmic bios get serialnumber
- Regkey
  - HARDWARE\Description\System (SystemBiosVersion)
  - HARDWARE\Description\System\BIOS (SystemManufacturer)
  - HARDWARE\Description\System (VideoBiosVersion) : Virtualbox
  - HARDWARE\Description\System (SystemBiosDate)

Process detection: checking for existence of specific processes in the windows process link list

Analysis tool	Process name	Details
VMWare Workstation	vm3dmp.sys, vmusbmouse.sys,Vmhgfs.sys, vmwareuser.exe, vmtoolsd.exe, vmmouse.sys	Vmmouse is the mouse driver of vmware installed on guest, part of VMWare tools service
Virtualbox	vboxguest.sys, vboxmouse.sys, vboxsf.sys, vboxvideo.sys, Vboxservice.exe, vboxtray.exe	
Sandbox IE	Sbiesvc.exe, sbiedll.exe, sbiectrl.exe	
Virtual PC	Vpcmap.exe, vmsrvc.exe	Virtual Machine Additions, Virtual Pc Integration Components
Xen	xenservice.exe	

Process Detection: malware sample distribution based on anti-vm process detection





CPU count: different ways used by malware samples to detect BIOS remained artifacts

- KVM:
  - <vcpu placement='static'>2</vcpu>
- Virtualbox
  -
- VMWare:
  - numvcpus = "4"

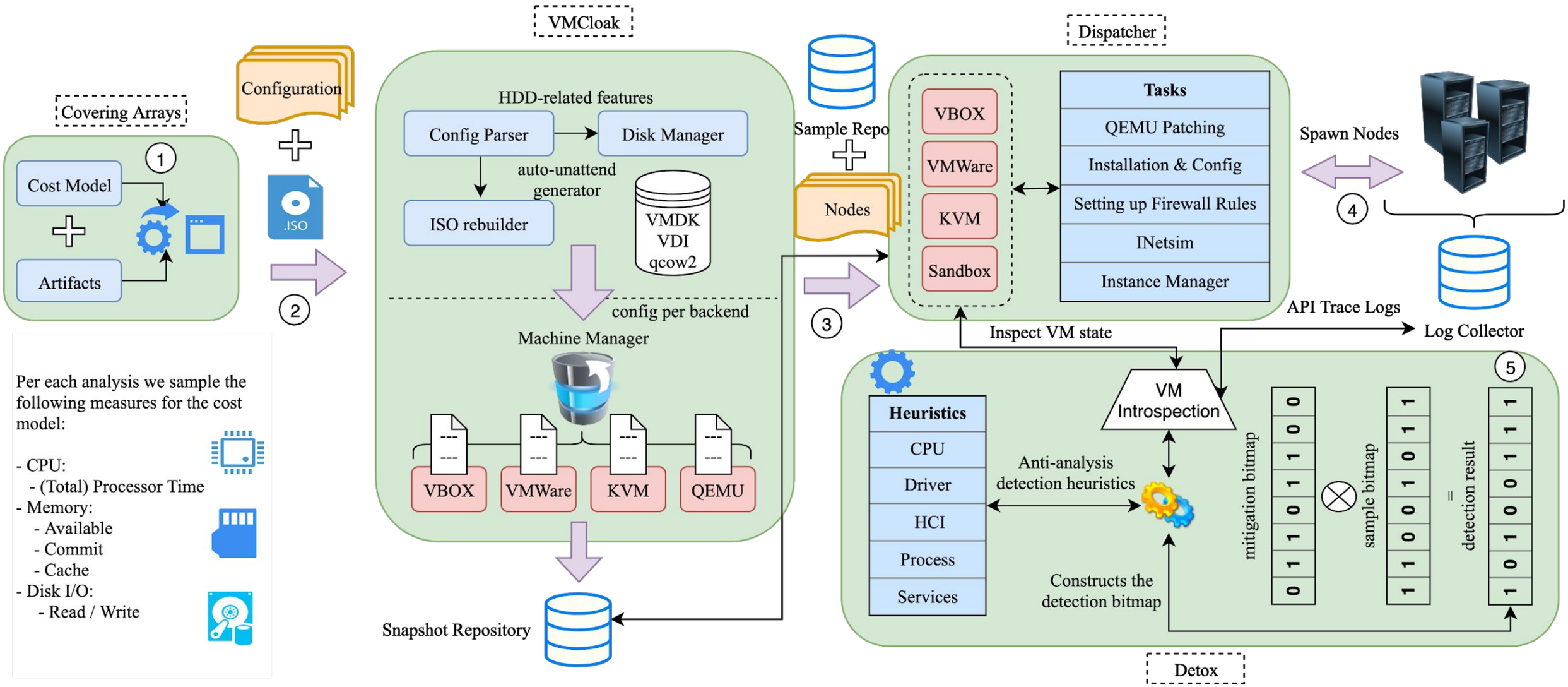
CPUID: there are two different ways employed to detect hypervisor using cpuid instruction:

1. checking hypervisor bit set in cpuid result ((ecx >> 31) & 0x1)
2. setting EAX=0x40000000, check result in strcat(EBX,ECX,EDX)

- KVM:
  - <vcpu placement='static'>2</vcpu>
- Virtualbox
  - <Paravirt provider="None"/>
  - Directly setting the bit (haven't tried this)
- VMWare:
  - hypervisor.cpuid.v0 = "FALSE"

Index	Hypervisor	Vendor name
1	VMWare	VMwareVMware
2	Parallels	prl hyperv
3	KVM	KVMKVMKVM\0\0\0
4	VirtualBox	VBoxVBoxVBox
5	Xen	XenVMMXenVMM
6	Virtual PC	Microsoft Hv

MIMOSA pipeline: A high-level overview of the framework



Per each analysis we sample the following measures for the cost model:

- CPU:
  - (Total) Processor Time
- Memory:
  - Available
  - Commit
  - Cache
- Disk I/O:
  - Read / Write