Статья Создание локального Runtime чекера антивирусами.

🚽 xss.is/threads/33978

Статья не новая(год ей), но как автор перепубликую ее тут.

Создание локального Runtime чекера антивирусами.

Все привет, наконец то я нашел время и как обещал выкладываю стать о том как сделать чекера на динамические детекты антивирусов (Runtime Detect Checker) на локальной машине.

Я сделал этот проект два годна назад, т.к. мне было жалко платить подобным сервисам, да и редко надо. Писал я для себя на питоне со своими нюансами, в нашем же случаи для статьи я сделал проще на bat-никах. И самое интересно мне друзья дали еще чужие исходники на php, где написан сервис на подобии как у меня на Python'е с тем же принципом, что в статье. И так все по порядку.

и так все по порядку

о. Методика

Вся суть методики: скоростное и эффективное создание одноразовых виртуальных машин с антивирусами на основе шаблонов, независимой заливкой файла и его запуском. Определение детектов происходит на основе скриншотов.

1. Ставим виртуальную машину.

Мы будем использовать виртуальную машину Virtual Box версии 5.28.8 x64 (обращаю ваше внимание, что API может отличаться в зависимости от релизов) на в операционной системе Windows(можно и на Linux, но локалка у меня виндовская). 1.png



Выбираем x64 версия для Windows, скачиваем VirtualBox тут http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html

2. Создаем шаблон ОС

Я делал виртуальную машину на Win7x64 и на Win10x64 потому что многие антивирусы ниже семерки уже не поддерживаются, да и с Win7 недавно натолкнулся на проблемы. Если машина позволяет рекомендую Windows 10 x64. Хотел бы обратить внимание на то что процессор должен поддерживать аппаратную виртуализцию VT-x/AMD-V (https://ru.wikipedia.org/wiki/ Аппаратная_виртуализация) и Hyper-threading (https://ru.wikipedia.org/wiki/Hyperthreading), проверьте чтобы было включено в Bios'e. У меня Intel i7 на 3800Гц 8 ядер. Если у вас нету хардварной виртуализции, то думаю статья эта вам не поможет, т.к. ВМ и сам компьютер будут ужасно тормазить и смысла ставить BM нету. Так же стоит заранее позаботиться о свободном месте на жестком диске HDD(идеально

Так же стоит заранее позаботиться о свободном месте на жестком диске HDD(идеально конечно SSD), я рекомендую не менее 300Гб и желательно на

отдельном жестком диске от основной операционной системы (иначе есть шанс ВМ

будут "давить" на жесткий диск, что будет отдавать на основную ОС). Про оперативную память - должно хватить 8Гб, но желательно иметь 16Гб.

Настраиваем месторасположения всем ВМ

2.png

3.png

🦸 Oracle VM VirtualBox Менеджер Файл Машина Справка 0 роить Сбросить Показать Созд Создать ٨ Exploit 9 9 🔘 Выключена Сделать Удалить Test_Ubuntu Имя 🕚 Выключена 🔷 Текущее сост Test_Win64 🔘 Выключена Test_Win7_32 🕺 Сохранена

🧃 Oracle VM VirtualBox Менеджер

Фай	л Машина Справка			
Þ	Настройки	Ctrl+G	1	
n	Импорт конфигураций	Ctrl+I		Спинки 😞
R	Экспорт конфигураций	Ctrl+E		
6 7	Менеджер виртуальных носителей	Ctrl+D	s XP (32-	bit)
5	Менеджер сетей хоста	Ctrl+W		
2	Менеджер сетевых операций		IAMOTH'	2048 M5
G	Проверить обновления		Girbinor	2
	Разрешить все сообщения		зки:	Гибкий диск, Оптический диск,
\checkmark	Выход	Ctrl+Q		Жесткий диск VT-x/AMD-V, Nested
64	_Test_Win7_64 (Связная ба)	📃 Дисплей	i	

Для создания BM(виртуальной машины) надо запустить VirtualBox и нажать на иконку 4.png

🏈 VirtualBox - Hact	ройки		?	\times
📃 Общие	Общие			
🧼 Ввод	Папка для машин по умолчанию:	E:\VirtualBox		~
Обновления	Библиотека аутентификации VRDP:	VBoxAuth		~
🌍 Язык				
📃 Дисплей				
🗗 Сеть				
💋 Плагины				
Прокси				
		ОК	Отме	на

Выставляем название основного шаблона AV_main на нем мы настроим ОС и потом клонируем на шаблоны для антивирусов.

			? >	<
~	Создать	виртуальную машину		
	-Укажите	имя и тип ОС		_
	Имя:	AV_main]
	Тип:	Microsoft Windows	- 64	
	Версия:	Windows 7 (64-bit)	•	
	Укажите	объём памяти		
			4096 🜩 ME	5
	4 MB	16384 ME	5	
	Жесткий	і диск		
	🔿 Не по	одключать виртуальный жёсткий диск		
	🖲 Созд	ать новый виртуальный жёсткий диск		
	🔿 Испо	льзовать существующий виртуальный жёсткий диск		
	R	Win7_64.vdi (Обычный, 25,00 ГБ)	× 🗔	
				_
		Подробный режим Создать	Отмена	

Ничего не трогаем, жмем Создать. После создания ВМ, находим ее в списке, выбираем и правой клавишей мышки на ней переходим в Настройки ВМ. 6.png

Расположение	
AV_main	
Размер	
	32,00 ГЕ
1 1 1 1 1 1 1 1 1 1 1	
4,00 Mb	2,00 16
Укажите тип	Укажите формат хранения
VDI (VirtualBox Disk Image)	Динамический виртуальный жёсткий диск
🔿 VHD (Virtual Hard Disk)	О Фиксированный виртуальный жёсткий диск
O VMDK (Virtual Machine Disk)	Разделить на файлы размером до 2х ГБ
O HDD (Parallels Hard Disk)	
O QCOW (QEMU Copy-On-Write)	

7.png

64	AV main (main)		🔛 Аудио		
17	Сохранена	0	Частроить	Ctrl+S	
64	AV_microsoft (main	Ģ	клонировать	Ctrl+O	
27	🛃 Сохранена	8	Удалить	Ctrl+R	
64	AV panda (main)	2	Сгруппировать	Ctrl+U	

В настройках выбираем носители и в IDE контроллере выбираем Оптический привод, находим iso образ с установщиком Windows (в нашем случае это будет Win7x64) 8.png

🥝 AV_main - Настройки			?	×	•
📃 Общие	Носители				ты
📰 Система	Носители	Атрибуты			
Дисплей	VBoxGuestAdditions.iso	оптический привод.	Живой CD/DVD	à	Выбрать образ оптического диска
😥 Носители	😤 Контроллер: SATA	Информация	Образ	-	Привод хоста 'D:'
炉 Аудио	AV_main.vdi	Размер:	55,29 MB		CentOS-6.9-x86_64-minimal.iso
Сеть		Расположение: Подсоединён к:	AV_main, AV_avg (mai		CentOS-6.5-i386-minimal.iso
у сом-порты					Изъять диск из привода
Общие папки					
📰 Интерфейс пользователя					
	\$ \$ B B				K
			ОК Отмен	a	5

В настройках выбираем сеть и оставляем Не подключен, чтобы ОС не смогла обновиться и не смогла отсылать данные. Жмем ОК, настройка самой ВМ готова. 9.png

🥝 AV	_main - Настройки		? ×
	Общие	Сеть	
	Система	Адаптер <u>1</u> Адаптер <u>2</u> Адаптер <u>3</u> Адаптер <u>4</u>	
	Дисплей	Включить сетевой адаптер	
\bigcirc	Носители	Тип <u>п</u> одключения: Не подключен 🔻	
	Аудио	Имя: 2	~
₽	Сеть		
	СОМ-порты		
Ø	USB		
	Общие папки		
=	Интерфейс пользователя		
			0779797
		OK	Отмена

Запускаем ВМ 10.png

🗿 Oracle VM VirtualBox Менеджер Файл <u>М</u>ашина Справка 👼 Снимки Сбросить Запус Настроить Создать Запустить А 64 AV_main (main) Общие 🕹 Сохранена Имя: AV_main OC: Windows 7 (64-bit) AV microsoft (main)

3. Настраиваем шаблон ОС

Должно появиться окно BM с установкой Windows, ставим как обычно, НО:

ВАЖНО!!! Имя юзера Admin пароль 12345

После установки, необходимо ввести лицензию/кряк/кейген - на ваше усмотрение, но чтобы приложение которое лицензирует не висело в памяти, а то AB его прихлопнут. Для ускорения работы BM отключаем всякий трешь.

Отключаем службы: обновления, индексации файлов, кэширования и т.д.

11.png

	Hanstorstill States	nacomacie yo m	cocarby scom
🔍 Security Cei <u>tt</u> er	The WSCS	Automatic (D	Local Service
🤹 Software Protection	Enables th	Disabled	Network S
🤐 Windows Defender	Protection	Disabled	Local System
🤍 Windows Font Cache Service	Optimizes	Disabled	Local Service
🤹 Windows Search	Provides c	Disabled	Local System
🤍 Windows Update	Enables th	Disabled	Local System
🤹 BranchCache	This servic	Disabled	Network S
🔍 Google Update Service (gupdate)	Keeps your	Disabled	Local System
🔍 Google Update Service (gupdatem)	Keeps your	Disabled	Local System
🔍 Internet Connection Sharing (ICS)	Provides n	Disabled	Local System
🔍 Media Center Extender Service	Allows Med	Disabled	Local Service
🔍 Microsoft .NET Framework NGEN v2.0.50727_X64	Microsoft	Disabled	Local System
🔍 Microsoft .NET Framework NGEN v2.0.50727_X86	Microsoft	Disabled	Local System
🔍 Net. Tcp Port Sharing Service	Provides a	Disabled	Local Service
🔍 Routing and Remote Access	Offers rout	Disabled	Local System
🧠 Superfetch	Maintains a	Disabled	Local System

В альтернативных настройка, отключаем бэкапы

ystem Properties	X
Computer Name Hardware Advanced	System Protection Remote
Use system protection to undo un restore previous versions of files.	wanted system changes and What is system protection?
System Restore	
You can undo system changes by revertin your computer to a previous restore point.	g System Restore
Protection Settings	Protection
Local Disk (C:) (System)	Off
Configure restore settings, manage disk s and delete restore points.	space, Configure
To create a restore point, first enable pro by selecting a drive and clicking Configu	tection <u>Create</u>
ОК	Cancel Apply

Ставим ускорение графики GUI 13.png

Syste	em Properties	×	
Co	mputer Name Hardware Advanced System Protection Remote		
	Performance Options Visual Effects Advanced Data Execution Prevention Select the settings you want to use for the appearance and performance of Windows on this computer.	×	
Г	C Let Windows choose what's best for my computer		
	Adjust for best performance Custom:		
	 Animate controls and elements inside windows Animate windows when minimizing and maximizing Animations in the taskbar and Start Menu Fade or slide menus into view Fade or slide ToolTips into view Fade out menu items after clicking Show shadows under mouse pointer Show shadows under windows Show translucent selection rectangle Show window contents while dragging Slide open combo boxes Smooth edges of screen fonts Smooth-scroll list boxes Use drop shadows for icon labels on the desktop 		3.6 ispla
	OK Cancel Apply		

Убиваем удаленного помощника

System Properties	×
Computer Name Hardware Advanced System Protection Remote	
Remote Assistance	
What happens when Lenable Remote Assistance?	
Advanced	
Remote Desktop	
Click an option, and then specify who can connect, if needed.	
 Don't allow connections to this computer 	
 Allow connections from computers running any version of Remote Desktop (less secure) 	
 Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure) 	
Help me choose Select Users	
UK Cancel Apply	

Mонтируем iso образ с VirtualBox Addons, устанавливаем драйвера и приложение VirtualBox Agent, если установка не началась то запустите вручную 17.png



🐝 AV_main (main) [Работает] - Oracle VM VirtualBox

Файл	Машина	Вид	Ввод	Устрой	ства	Справка		
				 Or 	тиче	ские диски	•	
				🖣 Ау	дио		•	
Compi	iter			🗗 Ce	ть		•	
				🤌 US	В		•	
L	2			iii 06	іщие	папки	•	
63	/			06	іщий	буфер обмена	•	
Recycle	e Bin			🛐 Фу	нкци	я Drag and Drop	•	
				🖉 По	дклн	чить образ диска Дополнений гостевой ОС		
Control	Panel							

После установки и перезагрузки у вас появится значок приложения, значит вы все правильно сделали 16.png

Я еще установил Chrome для того чтобы потом на образах ВМ было легче антивирусы качать, только не забудте отключить службу обновления Хрома. Для скачивания я настроил 18.png

и подключил сеть 19.png

После всех установок надо отключить сеть, чтобы данные не утекали. Ну вот в принципе и готов шаблон ВМ с ОС, отключаем ВМ в Сохраненном состоянии, это даст нам существенное ускорение при запуске.

20.png

Oracle VM VirtualBox Guest Additions 5.2.8r Pr 🌂 Խ 🔛 🕪 11:49, 5/27/20



21.png

4. Клонирование шаблона

Выбираем наш шаблон и правым кликом мыши жмем Клонировать. 22.png



🜃 AV_main (main) [Работает] - Oracle VM VirtualBox



		🌃 Закрыть виртуальную машину 🤉 🛛 🗙
		 ы хотите: ○ Сохранить состояние машины ○ Послать сигнал завершения работы ○ Выключить машину Восстановить текущий снимок 'main' ОК Отмена
وَنَ اللهُ على اللهُ اللهُ اللهُ اللهُ اللهُ اللهُ اللهُ اللهُ على اللهُ اللهُ مُحَاللهُ على اللهُ مُحَاللهُ على اللهُ اللهُ مُحَاللهُ على اللهُ مُحَاللهُ على اللهُ مُحَاللهُ مُحَاللهُ على اللهُ مُحَاللهُ مُحَاللهُ على اللهُ مُحَاللهُ مُحَاللهُ على اللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ على اللهُ مُحَاللهُ على اللهُ مُحَاللهُ مُحَاللهُ حَاللهُ على مُحَاللهُ مُحَاللهُ على مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ حَاللهُ حَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ حَاللهُ مُحَاللهُ مُحَاللهُ حَاللهُ مُحَالل	Y 🕹	-
Создать Настроить	Сбросить Запустить	
Создать Настроить Sea V_main (main Coxpanena	Сбросить Запустить	📃 Общие
Создать Настроить	Сбросить Запустить) ^ ^ Настроить	Общие Ctrl+S
Создать Настроить 4 Avmain (main Сохранена 4 Сохранена 4 Cохра	Сбросить Запустить) Линировать.	Сtrl+S Ctrl+O
Создать Настроить Создать Настроить Сохранена Сохро	Сбросить Запустить Мастроить <u>И</u> астроить <u>У</u> далить	Сtrl+S Ctrl+O Ctrl+R

Подписываем новую BM (AV_avg, AV_avira, AV_kis и т.д.)- это будет шаблон BM с антивирусом, в нашем случае я выбрал AVG. 23.png



2	~
£	

Клонировать виртуальную машину

Укажите тип клонирования					
Пожалуйста укажите какое клонирование Вы желаете выполнить.					
Если Вы выберите Полное клонирование , будет создана полная копия клонируемой виртуальной машины (включая все файлы виртуальных жёстких дисков).					
Если Вы выберите Связное клонирование , будет создана новая машина, использующая файлы виртуальных жёстких дисков клонируемой машины и Вы не сможете перенести новую машину на другой компьютер без переноса клонируемой.					
Если Вы выберите Связное клонирование , в клонируемой машине также будет создан новый снимок, являющийся частью процедуры клонирования.					
Полное клонирование					
О <u>С</u> вязное клонирование					
<u>Д</u> алее Отмена					

И так создаем все шаблоны ВМ для каждого антивируса который нам надо.

5. Установка АВ на шаблоны

После создания запускаем по очереди все виртуальные машины и на каждую ставим антивирус.

ВАЖНО!!!: Незабываем включить сеть и после установки отключить, а ТАКЖЕ выключить BM с AB в Сохраненном состоянии.

6. Создание срезов

После подготовки шаблонов BM с AB надо создать срезы (snapshot) - это фиксирование состояния BM для создания Связанной копии. Что это дает, это дает нам быстрое создание копии BM из шаблона с нужным нам AB, быстрый старт AB, проверку ехе и быстрое удаление BM без нагрузки на HDD/SDD

Срезы надо делать после обновления АВ в шаблонах.

ВАЖНО!!! Перед созданием среза, убедитесь что остальные срезу удалены, иначе будут ошибки. На каждом шаблоне ВМ с АВ должен быть один срез с названием - "main"

Срезы можно создать руками или автоматом. **руками:** выберете шаблон ВМ с АВ и создайте срез 25.png

🧊 Ora	cle VM Virtua	alBox Менед	жер				—		×
<u>Ф</u> айл	<u>М</u> ашина	Справк <u>а</u>							
		\checkmark	\Rightarrow	•	🔄 Снимки 🗯	🗐 Детали 🗯	<i>~</i> -		
Создать	Настроить	Сбросить	Запустить		~~~~~		Машины	Инструме	нты
64	AV_avg (mair	r)	^	📃 Общие) [Превью			
	🚭 Сохранен	a		Имя: AV_avg	(
64	AV avira (ma	ain)		OC: Windows 7 (64-bit)		-00 			
17	🔁 Сохранен	a		🚺 Система		411			

26.png



27.png

🐧 Сде	лать снимок виртуальной машины	?	\times
64	Имя снимка		
	Описание снимка		
	ОК Отмена	Справн	ka

автоматом: для этого я создал bat файт _create_snapshot.bat(перед созданием BCE AB должны быть выключены) и для удаления всех срезов _del_snapshot.bat(перед удалением BCE AB должны быть выключены)

T.e. еще раз повторюсь, срезы надо пересоздавать когда вы обновите антивирусы на шаблонах BM с AB, должен быть только один срез с названием "main", перед пересозданием все BM должны быть выключены.

7. Первый запуск

Все шаблоны с AB созданы, настроены, обновлены антивирусы, инет на них отключен, они выключены в Сохраненном состоянии, срезы сделаны.

Переходим к самой важной части - тестированию

Я подготовил bat файлик _start.bat как пример тестирования, тестировать мы будем hello.exe (мессажебокс)

Code:

```
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" clonevm AV_avg --snapshot main --name
AV avg tmp --register --options link
TIMEOUT 5
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm AV avg tmp
TIMEOUT 40
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV avg tmp copyto
"C:\dynamic_check\hello.exe" --target-directory "C:\Users\Admin\AppData\Local\Temp" --
username "Admin" --password "12345" --verbose
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV avg tmp start --exe
"C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" --password "12345" --verbose
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV avg tmp screenshotpng
"src avg 1.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng
"src avg 2.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV avg tmp screenshotpng
"src avg 3.png"
TIMEOUT 3
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV avg tmp screenshotpng
"src avg 4.png"
TIMEOUT 1
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV avg tmp poweroff
TIMEOUT 5
"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" unregistervm AV_avg_tmp --delete
```

Теперь поясню каждую строку

clonevm AV_avg --snapshot main --name AV_avg_tmp --register --options link делаем связанное клонирование шаблон BM с AB с именем AV_avg используя срез "main" название новой одноразовой BM AV_avg_tmp

startvm AV_avg_tmp

старт одноразовой ВМ AV_avg_tmp

guestcontrol AV_avg_tmp copyto "C:\dynamic_check\hello.exe" --targetdirectory "C:\Users\Admin\AppData\Local\Temp" --username "Admin" -password "12345" --verbose

копируем наш тестовый файл "C:\dynamic_check\hello.exe" указанием полного пути в гостевую одноразовую BM AV_avg_tmp в папку "C:\Users\Admin\AppData\Local\Temp" использую учетную запись Admin

guestcontrol AV_avg_tmp start --exe "C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" -password "12345" --verbose

запускаем наш "hello.exe" на одноразовой гостевой BM AV_avg_tmp использую учетную запись Admin

controlvm AV_avg_tmp screenshotpng "src1.png"

создания скриншотов гостевой одноразовой BM AV_avg_tmp

controlvm AV_avg_tmp poweroff

отключаем принудательно питание гостевой одноразовой BM AV_avg_tmp

unregistervm AV_avg_tmp --delete

удаляем гостевую одноразовую BM AV_avg_tmp из списка с удалением файла BM

Если все сделали правильно у вас в консоли будет такой лог и появятся скриншоты, а на экране одноразовой BM AV_avg_tmp будет такое окно 30.png



Далее вы можете анализировать скриншоты. Таймауты стоят относительные, вы сами можете с ними играться.

Консольный лог Code: C:\dynamic check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" clonevm AV avg -snapshot main --name AV avg tmp --register --options link Machine has been successfully cloned as "AV_avg_tmp" C:\dynamic check>TIMEOUT 5 Время ожидания 5 сек., нажмите любую клавишу для продолжения ... C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm AV_avg_tmp Waiting for VM "AV avg tmp" to power on... VM "AV_avg_tmp" has been successfully started. C:\dynamic check>TIMEOUT 40 Время ожидания 40 сек., нажмите любую клавишу для продолжения ... C:\dynamic check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV avg tmp copyto "C:\dynamic_check\hello.exe" --target-directory "C:\Users\Admin\AppData\Local\Temp" -username "Admin" --password "12345" --verbose Creating guest session as user 'Admin'... Waiting for guest session to start... Successfully started guest session (ID 1) Copying from host to guest ... Directory "C:\Users\Admin\AppData\Local" already exists Source: C:\dynamic check\hello.exe Copying "C:\dynamic_check\hello.exe" to "C:\Users\Admin\AppData\Local\Temp" ... Closing guest session ... C:\dynamic check>TIMEOUT 3 Время ожидания 3 сек., нажмите любую клавишу для продолжения ... C:\dynamic check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" guestcontrol AV avg tmp start --exe "C:\Users\Admin\AppData\Local\Temp\hello.exe" --username "Admin" --password "12345" --verbose Creating guest session as user 'Admin'... Waiting for guest session to start... Successfully started guest session (ID 1) Starting guest process ... [4076 - Session 1] Process successfully started! Guest session detached C:\dynamic check>TIMEOUT 3 Время ожидания 3 сек., нажмите любую клавишу для продолжения ... C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng "src1.png" C:\dynamic check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng "src2.png"

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng "src3.png"

C:\dynamic_check>TIMEOUT 3

Время ожидания 3 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp screenshotpng "src4.png"

C:\dynamic_check>TIMEOUT 1

Время ожидания 1 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm AV_avg_tmp poweroff

C:\dynamic check>TIMEOUT 5

Время ожидания 5 сек., нажмите любую клавишу для продолжения ...

C:\dynamic_check>"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" unregistervm AV_avg_tmp --delete

Так же вкалдываю сонсольны хелп Code: Usage:

```
VBoxManage guestcontrol
                            <uuid vmname> [--verbose -v] [--quiet -q]
                              [--username <name>] [--domain <domain>]
                              [--passwordfile <file> | --password <password>]
                              run [common-options]
                              [--exe <path to executable>] [--timeout <msec>]
                              [-E|--putenv <NAME>[=<VALUE>]] [--unquoted-args]
                              [--ignore-operhaned-processes] [--profile]
                              [--no-wait-stdout|--wait-stdout]
                              [--no-wait-stderr|--wait-stderr]
                              [--dos2unix] [--unix2dos]
                              -- <program/arg0> [argument1] ... [argumentN]]
                              start [common-options]
                              [--exe <path to executable>] [--timeout <msec>]
                              [-E|--putenv <NAME>[=<VALUE>]] [--unquoted-args]
                              [--ignore-operhaned-processes] [--profile]
                              -- <program/arg0> [argument1] ... [argumentN]]
                              copyfrom [common-options]
                              [--dryrun] [--follow] [-R|--recursive]
                              <guest-src0> [guest-src1 [...]] <host-dst>
                              copyfrom [common-options]
                              [--dryrun] [--follow] [-R|--recursive]
                              [--target-directory <host-dst-dir>]
                              <guest-src0> [guest-src1 [...]]
                              copyto [common-options]
                              [--dryrun] [--follow] [-R|--recursive]
                              <host-src0> [host-src1 [...]] <guest-dst>
                              copyto [common-options]
                              [--dryrun] [--follow] [-R|--recursive]
                              [--target-directory <guest-dst>]
                              <host-src0> [host-src1 [...]]
                              mkdir|createdir[ectory] [common-options]
                              [--parents] [--mode <mode>]
                              <guest directory> [...]
                              rmdir|removedir[ectory] [common-options]
                              [-R|--recursive]
                              <guest directory> [...]
                              removefile|rm [common-options] [-f|--force]
                              <guest file> [...]
                              mv|move|ren[ame] [common-options]
```

```
<source> [source1 [...]] <dest>
                              mktemp|createtemp[orary] [common-options]
                              [--secure] [--mode <mode>] [--tmpdir <directory>]
                              <template>
                              stat [common-options]
                              <file> [...]
VBoxManage guestcontrol
                            <uuid|vmname> [--verbose|-v] [--quiet|-q]
                              list <all|sessions|processes|files> [common-opts]
                              closeprocess [common-options]
                                --session-id <ID>
                              <
                                --session-name <name or pattern>
                              <PID1> [PID1 [...]]
                              closesession [common-options]
                              < --all | --session-id <ID>
                                --session-name <name or pattern> >
                              updatega | updateguestadditions | updateadditions
                              [--source <guest additions .ISO>]
                              [--wait-start] [common-options]
                              [-- [<argument1>] ... [<argumentN>]]
                              watch [common-options]
```

8. Ошибки и литература

Если по какой то причине вы не смогли удалить срез - значит он еще привязан к ВМ, удалите ВМ который был клонирован связанно, в нашем случае все ВМ с названием *_tmp - их не должно быть.

ВАЖНО!!! Бывает по какойто причине ВМ *_tmp завершиласть некоректно, тогда надо удалить все ВМ *_tmp и удалить их файлы в папке где они храняться с названием *_tmp.

Иногда когда все удалено и ВМ выключены, пересоздать срез или ВМ *_tmp не возможно надо руками удалить носитель. Будте окуратнее

28.png

		<u>⊅</u> айл	<u>М</u> ашина	Справк <u>а</u>			
		۶ ۱	<u>Н</u> астройки	тройки		Ctrl+G	
		ุณ เ	<u>И</u> мпорт конфи	ігураций		Ctrl+I	
		Q :	<u>Э</u> кспорт конфи	игураций		Ctrl+E	
		<u>7</u> I	Менеджер вир	туальных н <u>о</u> си	птелей	Ctrl+D	
		<u> </u>	Менеджер с <u>е</u> те	ей хоста		હtrl+W	
		ا 🛓	Менеджер <u>с</u> етевых операций				
		<u>9</u>	<u>П</u> роверить обн	ювления			
		<u> </u>	<u>Р</u> азрешить все	сообщения			
		7	<u>В</u> ыход			Ctrl+Q	
имя					вирт. размер	wакт. размер	ľ
~	{359baa7c-3ad0-4342-9cf8-5c4b1fd3482a}.vdi				25,00 ГБ	409,00 ME	
	{96d8fd5b-c5c5-4d48-9918-c533e63551f9}.vdi				25,00 ГБ	2,00 ME	
	{375e5e04-3eef-4db0-93c7-b82dd7aa6eb6}.vdi				25,00 FE	10,61 FE	
>	{50bf2385-fbc9-436a-91cb-9fd6e171a586}.vdi				25,00 ГБ	1,94 ГБ	
>	{58e0f992-d9c0-4b58-806f-c842f72af6a6}.vdi				25,00 ГБ	1,18 ГБ	

25,00 ГБ

25,00 ГБ

25,00 ГБ

25,00 ГБ

2,27 ГБ

1,07 ГБ

2,53 ГБ

2,07 ГБ

> {58e0f992-d9c0-4b58-806f-c842f72af6a6}.vdi {6b3baeb4-fcbb-4894-baf0-54145a09be50}.vdi > {7811a7e4-bacf-4425-a462-d13de0267244}.vdi

> {93906adf-64cc-4ea6-8676-171ee915ebef}.vdi

> {97c9face-24f2-474c-a651-cfd71a0d59f4}.vdi

Если вы что то сделали не так смотрите ошибки и перечитывайте статью. Полное описание всех команд вы найдете на официальном сайте

https://www.virtualbox.org/manual/и https://www.virtualbox.org/manual/cho8.html.

9. Пояснения

имя

Азм постарался сделать как можно проще статью и примеры, чтобы было понятна сама методика Runtime проверки антивирусами, создания шаблонов и использования быстрого запуска.

Я не делал контроля запуска ВМ и ОС, так же не делал работу с сетью и запуск с использованием окружения - мне было лениво.

10. Подарок

Мне друзья для этой стать скинули исходники полноценного сервиса последовательной проверки на php, сервис использую примерно такую же методику, что я описал в статье. Если вы серьезный программист и вам понравилась статья, то можете поиграться с этим сервсим и реализовать свой.

Я правда считаю что пример в стать делать в виде массового сервиса не целесообразно, будет слишком огромное потребление ресурсов, для создания полноценного сервиса надо измениить подход и возможно использовать другие виртуальные машины к пример qemu, но суть методики останется та же.

11. Файлы

Ссылка:

https://mega.nz/#!IVgnoSDT!TLpiWj11SLanT57u6YOVI4bzupg63THIkrgZCM2IyIw Пароль: exploit.in

12. Дополнения

Хотелось бы немного сказать про антидетект виртуальной машины, а то мне тут целую истерику устроили, что такой проект и методику может любой сделать, и что я слишком много внимания уделил простым вещам, надо было про антидект лучше написать - смешно. По антидетекту все в инте есть, а вот подобных статей НЕТУ! По антидетекту

- есть замечательный опенсорс проект который чекает вм и показывает детекты https://github.com/aortega/pafish , там же есть бинарнник.

 - есть замечательный проект с патчером vbox для антиэмуляции, он и мышку эмулирует и имена устройств меняет, реестр правит, куча всего для того чтобы софт не мог детектить вашу виртуалку https://github.com/hfirefox/VBoxHardenedLoader
 - есть отличное сообщество http://www.kernelmode.info/forum/viewtopic.php?
 f=11&t=3478 где ребята обсуждают и дорабатывают патчер

В принципе больше по этой теме обсуждать нечего, все есть в наличии и в исходниках, но для их использования надо иметь скилл или делать еще одну статью.

Я много чего еще в этой статье не указал, потому что невозможно все охватить за раз, поэтому в задницу ваши претензии без внипетов и примеров.

PS: народ пожалейте мою психику, не задавайте в ЛС мне вопросы