Introduction

Ransomware has struck again — the victim, Wonky Chocolates.

An unknown actor has gained access to the Wonky Chocolates corporate network. They claim they have exfiltrated confidential company records and have left a ransom note stating they found 'something secret' and will be in touch with demands to prevent its release.

The Wonky Chocolates executive team are demanding answers.

As the Incident Responder for Wonky Chocolates, you will need to draw upon your knowledge and skills to validate these claims. This may include (but is not limited to) verifying:

- the actor gained access to the Wonky Chocolates network
- the actor exfiltrated confidential company records

but ultimately, can you save Wonky Chocolates by recovering their data?

Pre-requisites

*** Bring your own Laptop ***

This training is designed to prepare you for incident response. The first stage of Incident response is preparation and this course is designed to have you prepared to respond.

As such we will provide you with an environment that is suitable for the analysis of artefacts obtained during an incident, this will require that you bring your own laptop, and follow the instructions below to have the analysis environment setup and ready.

The course requires a powerful laptop that is capable of running a virtual machine and some of the tools can be CPU intensive.

Please see the Virtual machine section for details on how to prepare the required virtual machines for the course.

Due to the course requirements, the people running the course will only be able to provide best effort support in assisting with setup.

System Requirements

A laptop with the following requirements

- CPU: Recent generation processor with virtualisation technology (Some ARM chips are unsuitable).
- CPU Settings: Virtualisation technology enabled in the BIOS.
- RAM: 8GB minimum 16GB+ recommended.
- Hard drive: 50GB free space.
- Admin access to the machine, and permission to install new software / run virtual machines that may contain malicious content.

Virtual Machines

The course performs all of its work within the SIFT workstation built by SANS. This document will outline the entire process necessary to have the machine setup.

Enable Virtualisation within the BIOS

Virtualisation features within the CPU will need to be enabled to allow virtual machines to run within the operating system, this is different for each model of computer, please refer to your user manual for specific details with the following being a basic guide:

- Reboot your computer
- During the boot process, interrupt the boot to enter the bios.
- Enable Virtualisation. This is called VT-x for intel CPUs and AMD-V for AMD.

Due to the nature of this change, this change can not be made by the people running the course. Please ensure this enabled before arrival.

Installing Virtualisation Software

The training will be run using VirtualBox. This software is freely available.

- If using Windows, Download and install the Visual C++ Redistributable software from https://learn.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170#visual-studio-2015-2017-2019-and-2022

Once that is installed, Virtualbox can be downloaded and installed.

- Download and install VirtualBox from https://www.virtualbox.org/wiki/Downloads
- Optional: Download and install the Virtualbox Extension Pack. The link is available on the page above.

Download / Setup Virtual Machine

Once the hypervisor has been installed, there are two options to setup the virtual machines.

- Build your own environment, or
- Download a pre-built virtual machine.

Build your own SANS SIFT Workstation.

If you would like to build your own environment the following guide can be used. Each step is described in detail; however, you may need to adjust it for your environment

From your web browser

- Download Ubuntu 22.04 Desktop from https://ubuntu.com/download/desktop

Within Virtualbox

- Click New and enter the following details
- Under Name and Operating System
    - Name: SIFT Workstation – ACSC Training
    - ISO Image: Select the Ubuntu ISO downloaded above
    - Type: Ubuntu
    - Version: Ubuntu (64-bit)
    - Select ‘Skip Unattended Installation’
- Under Hardware
    - Base Memory: 4096 MB
    - CPU 2
- Under Hard Disk
    - Change size to 30GB or more

    - Hard Disk file type and variant: VMDK
- Select Finish.
- Once created, power on the machine and performed the install.
    - When prompted create a user with username ‘sansforensics’ and password of ‘forensics’
- Once installed, Install the Virtualbox guest additions
    - Run ‘sudo apt install gcc make perl’
    - Select Devices -> ‘Insert Guest additions CD image’
    - Select run to perform install.
- Install Cast
    - Visit releases on https://github.com/ekristen/cast
    - Download latest cast image and install by running `sudo dpkg -i cast_v0.14.0_linux_amd64.deb’
- Install SIFT
    - From terminal run `sudo cast install teamdfir/sift-saltstack`

Once installed successfully. Download the artefacts from https://filedrop.cyber.gov.au/link/PITjEO1rOOve86tzBeGgXU (Approx 700MB) and place them on the desktop.

Download a pre-build virtual machine

A prebuilt SIFT workstation with the ACSC artefacts already in place on the desktop can be downloaded from https://filedrop.cyber.gov.au/link/qPqjB9TZbzBLVA4eyH1pGS (Approx 9GB)

Once downloaded, from within Virtualbox,

- Select File -> Import Appliance
- Under Source select the downloaded OVA
- Expand Settings and untick ‘Import hard drives as VDI’
- Test boot the machine

User details

- Username: sansforensics
- Password: forensics

!! WARNING !!

Some of the files may contain malicious code. All of the files have protections in place to prevent them from being able to run automatically, however suitable precautions should be taken when working with such files.