Laboratory Exercise 1 – Detonation of Ransomware via the Cyber Range/Any-Run Sandbox

Due Date: 02/19/2023
Points Possible: 5 points.

1. Overview

This week we will perform malware analysis to explore how detonation of ransomware looks like. Ransomware is a type of malwares that holds the system for ransom by locking users out of their computer or by encrypting their files. That said, detonation/Analysis of a ransomware program requires a safe and secure lab environment, as you do not want to infect your system or the production system. For this lesson, students will learn how to use the Cyber Range and Any-Run cloud-based Sandbox. Furthermore, Any-Run Sandbox will be used specifically to complete basic tasks in order to detonate securely WannaCry ransomware file.

2. Resources required

This exercise requires a Kali Linux VM running in the Cyber Range and Any-Run Sandbox.

[Note: This lab exercise requires an account on the Cyber Range and an account on the Any-Run Sandbox. To sign up for an account on The Range and Sandbox, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

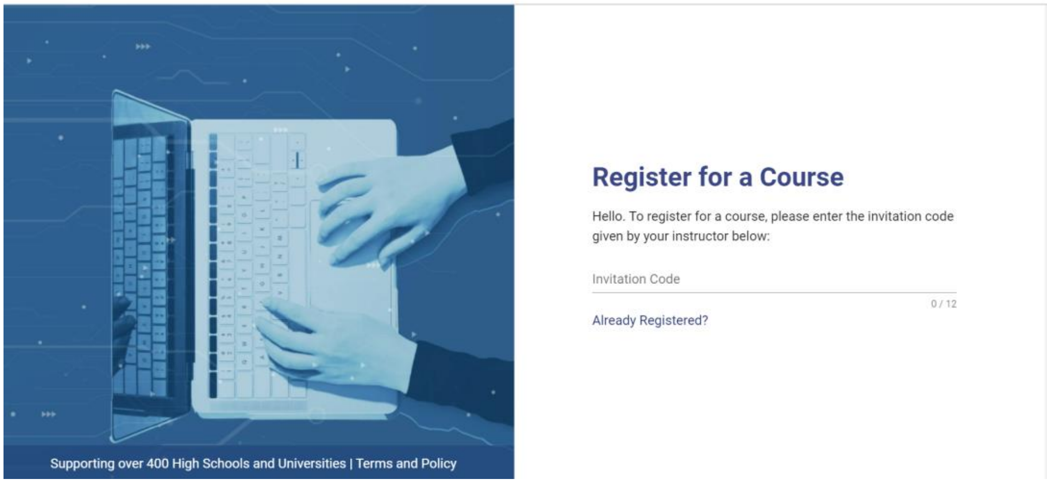
3. Initial Setup

1) For this exercise, first, you will log in to your Cyber Range account and select the Kali Linux, then click “start” to start your environment and “join” to get to your Linux desktop.
2) Second, you will download a WannaCry ransomware file from https://github.com/bill-zhanxg/WannaCry-Download and unzipped the downloaded ransomware file on the Kali Linux desktop of the Cyber Range account.
3) Third, you will log in to Any-Run Sandbox account and operate Malware Hunting platform, then click “New task” to start upload a WannaCry ransomware file.

4. Tasks

Task 1: Getting to the Kali Linux of your Cyber Range account

Open and access a Cyber Range account (using your Scranton email account) based on an invitation derived from the Cyber Range



Register for a Course

Hello. To register for a course, please enter the invitation code given by your instructor below:

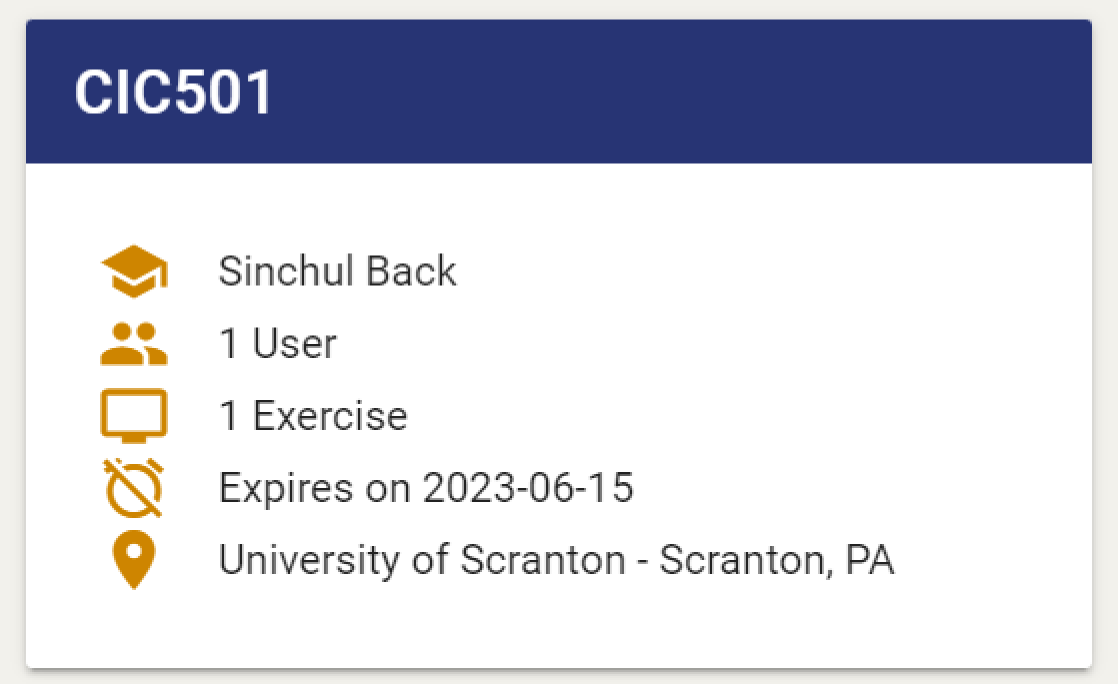
Invitation Code

0 / 12

Already Registered?

Supporting over 400 High Schools and Universities | Terms and Policy

Once you successfully log in the Cyber Range, the **Courses page** will appear. Then select and click “CIC501” course.



CIC501

Sinchul Back

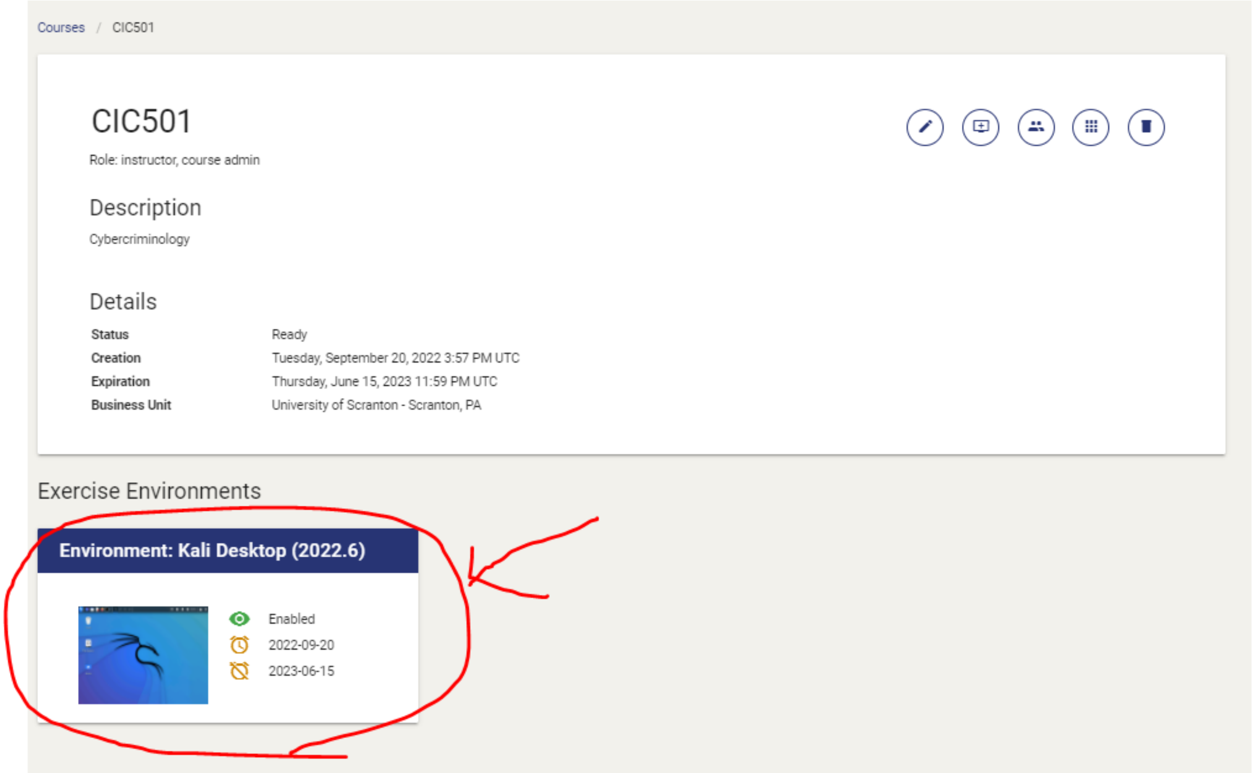
1 User

1 Exercise

Expires on 2023-06-15

University of Scranton - Scranton, PA

Select and click "Environment: Kali Desktop (2022.6)" course. Then click and open the Kali Linux Desktop.



Courses / CIC501

CIC501

Role: instructor, course admin

Description

Cybercriminology

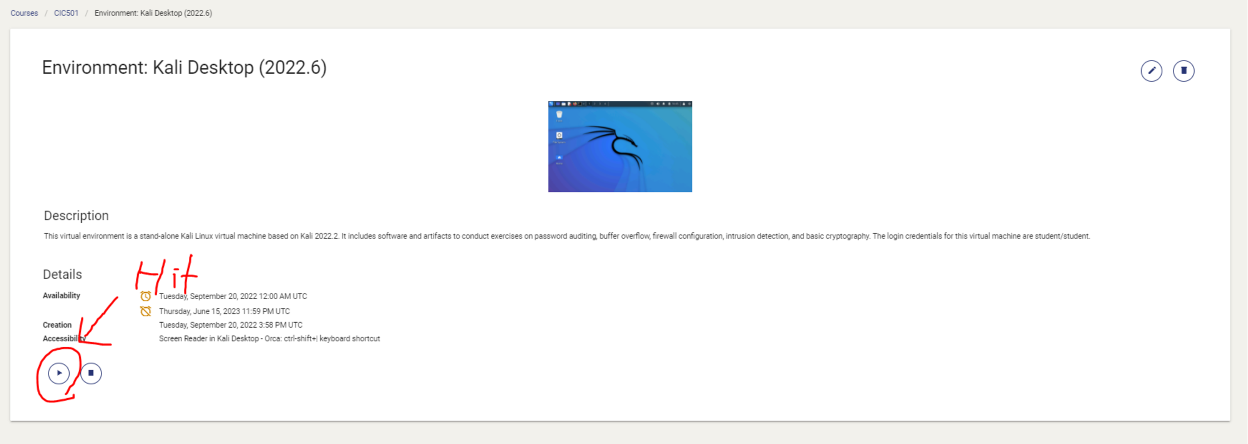
Details

Status	Ready
Creation	Tuesday, September 20, 2022 3:57 PM UTC
Expiration	Thursday, June 15, 2023 11:59 PM UTC
Business Unit	University of Scranton - Scranton, PA

Exercise Environments

Environment: Kali Desktop (2022.6)

Enabled
2022-09-20
2023-06-15



Courses / CIC501 / Environment: Kali Desktop (2022.6)

Environment: Kali Desktop (2022.6)

Description

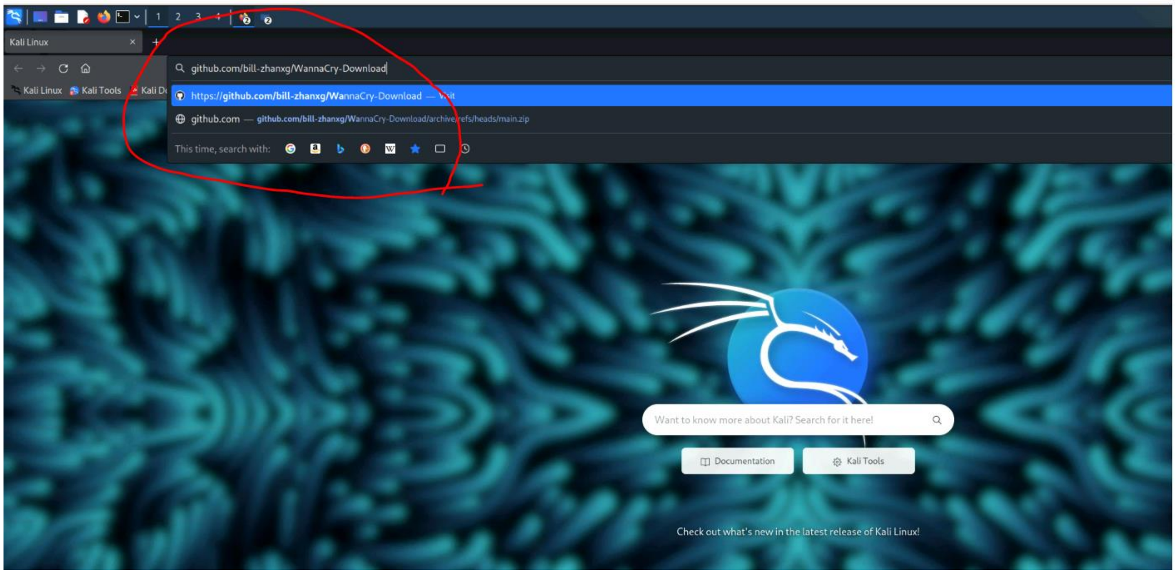
This virtual environment is a stand-alone Kali Linux virtual machine based on Kali 2022.2. It includes software and artifacts to conduct exercises on password auditing, buffer overflow, firewall configuration, intrusion detection, and basic cryptography. The login credentials for this virtual machine are student/student.

Details

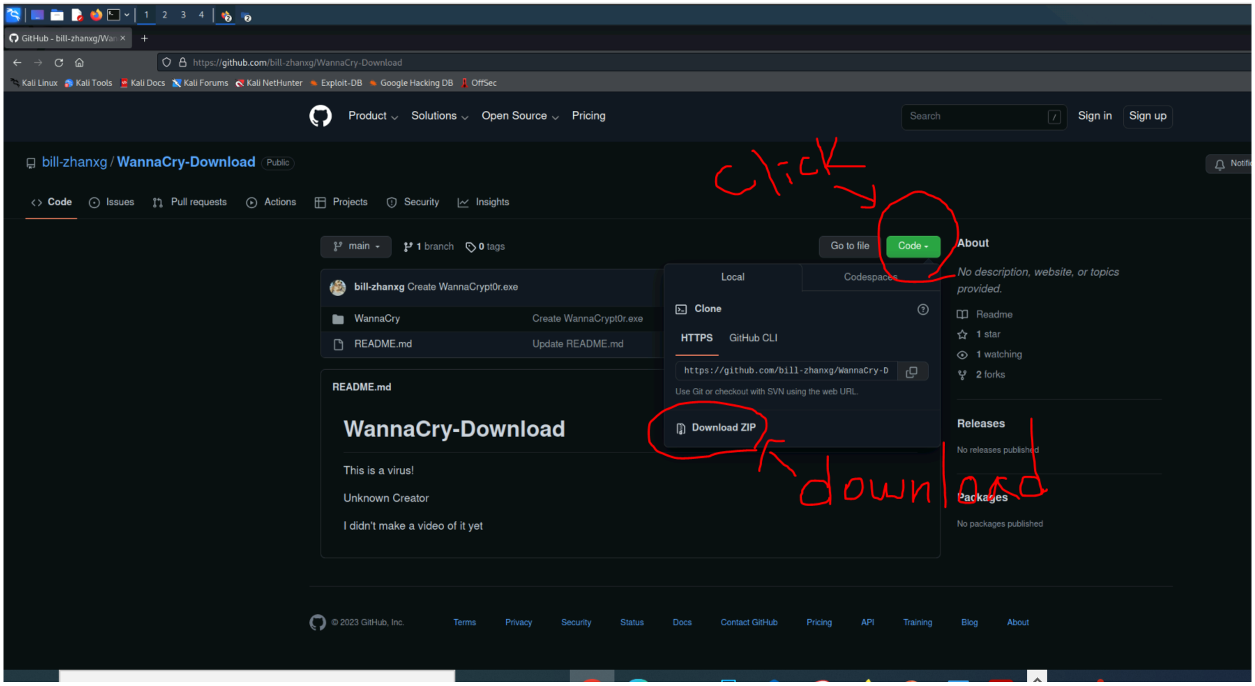
Availability	Tuesday, September 20, 2022 12:00 AM UTC Thursday, June 15, 2023 11:59 PM UTC
Creation	Tuesday, September 20, 2022 3:58 PM UTC
Accessibility	Screen Reader in Kali Desktop - Orca: ctrl-shift+| keyboard shortcut

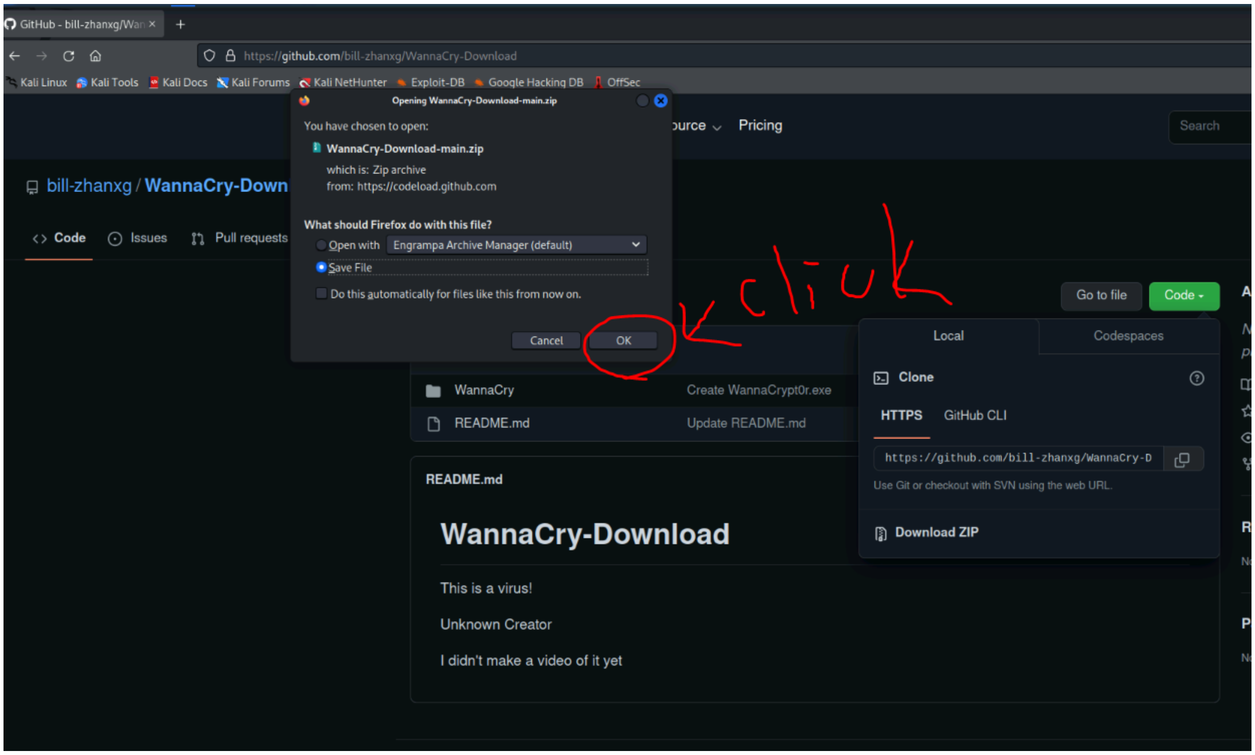
Task 2: Downloading a WannCry Ransomware file

Open a Firefox and type a web address: https://github.com/bill-zhanxg/WannaCry-Download. Click on **Close** at the bottom.


Kali Linux
github.com/bill-zhanxg/WannaCry-Download
https://github.com/bill-zhanxg/WannaCry-Download — Visit
github.com — github.com/bill-zhanxg/WannaCry-Download/archive/refs/heads/main.zip
This time, search with:
Kali Linux
Kali Tools
Want to know more about Kali? Search for it here!
Documentation
Kali Tools
Check out what's new in the latest release of Kali Linux!

You need download a WannaCry ransomware file from https://github.com/bill-zhanxg/WannaCry-Download and unzipped the downloaded ransomware file on the Kali Linux desktop of the Cyber Range account.





Opening WannaCry-Download-main.zip

You have chosen to open:

WannaCry-Download-main.zip

which is: Zip archive
from: https://codeload.github.com

What should Firefox do with this file?

○ Open with Engrampa Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

Cancel OK

```
https://github.com/bill-zhanxg/WannaCry-D
```

Use Git or checkout with SVN using the web URL.

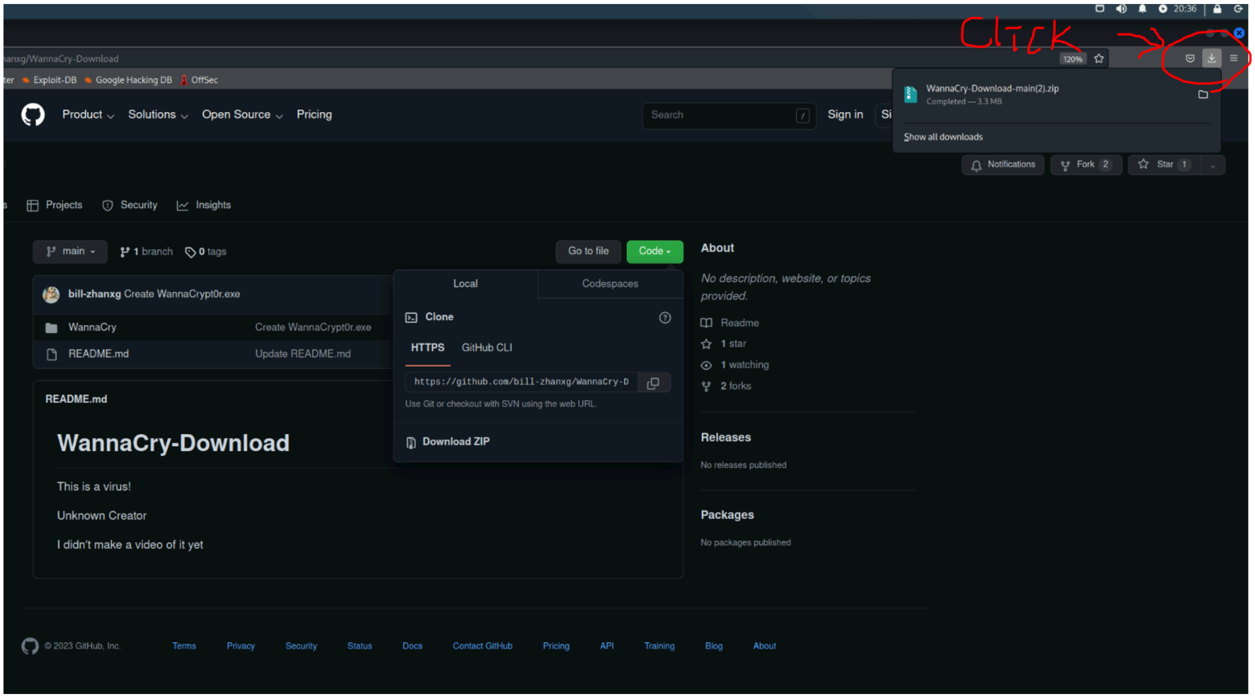
README.md

WannaCry-Download

This is a virus!

Unknown Creator

I didn't make a video of it yet



WannaCry-Download-main(2).zip
Completed — 3.3 MB

Show all downloads

bill-zhanxg Create WannaCrypt0r.exe

WannaCry Create WannaCrypt0r.exe

README.md Update README.md

```
https://github.com/bill-zhanxg/WannaCry-D
```

Use Git or checkout with SVN using the web URL.

No description, website, or topics provided.

No releases published

No packages published

README.md

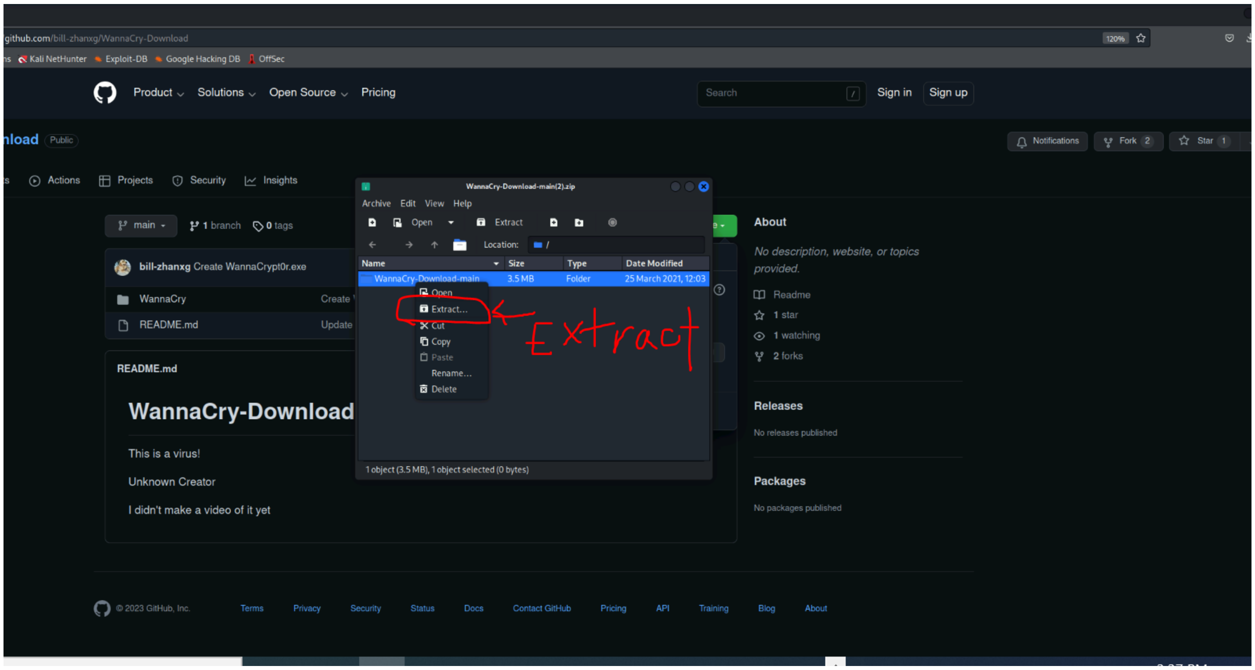
WannaCry-Download

This is a virus!

Unknown Creator

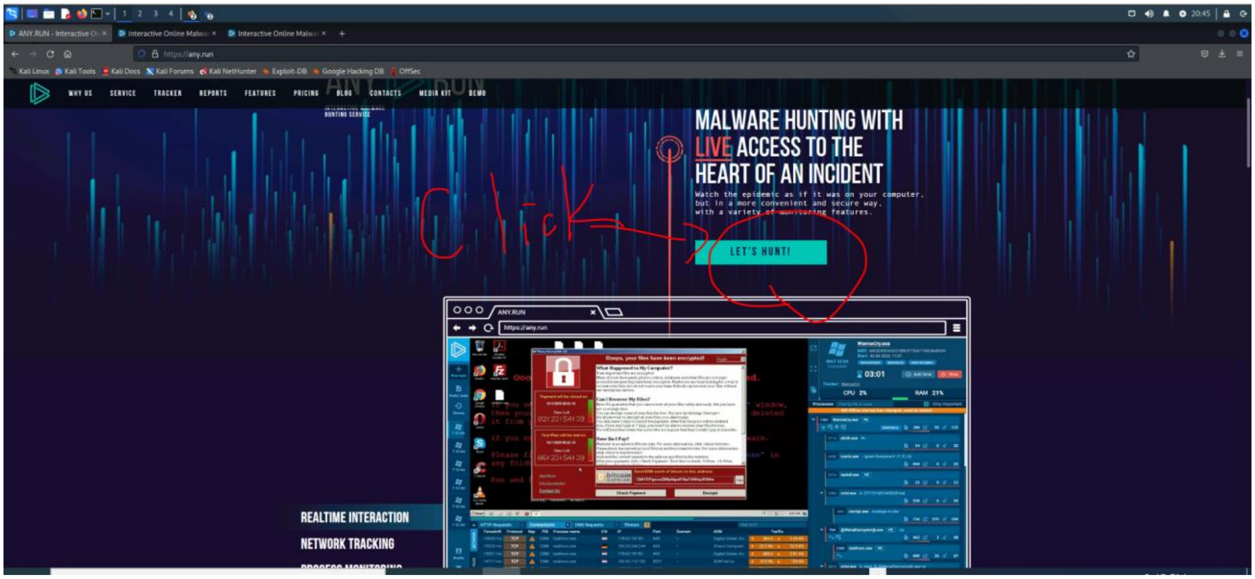
I didn't make a video of it yet

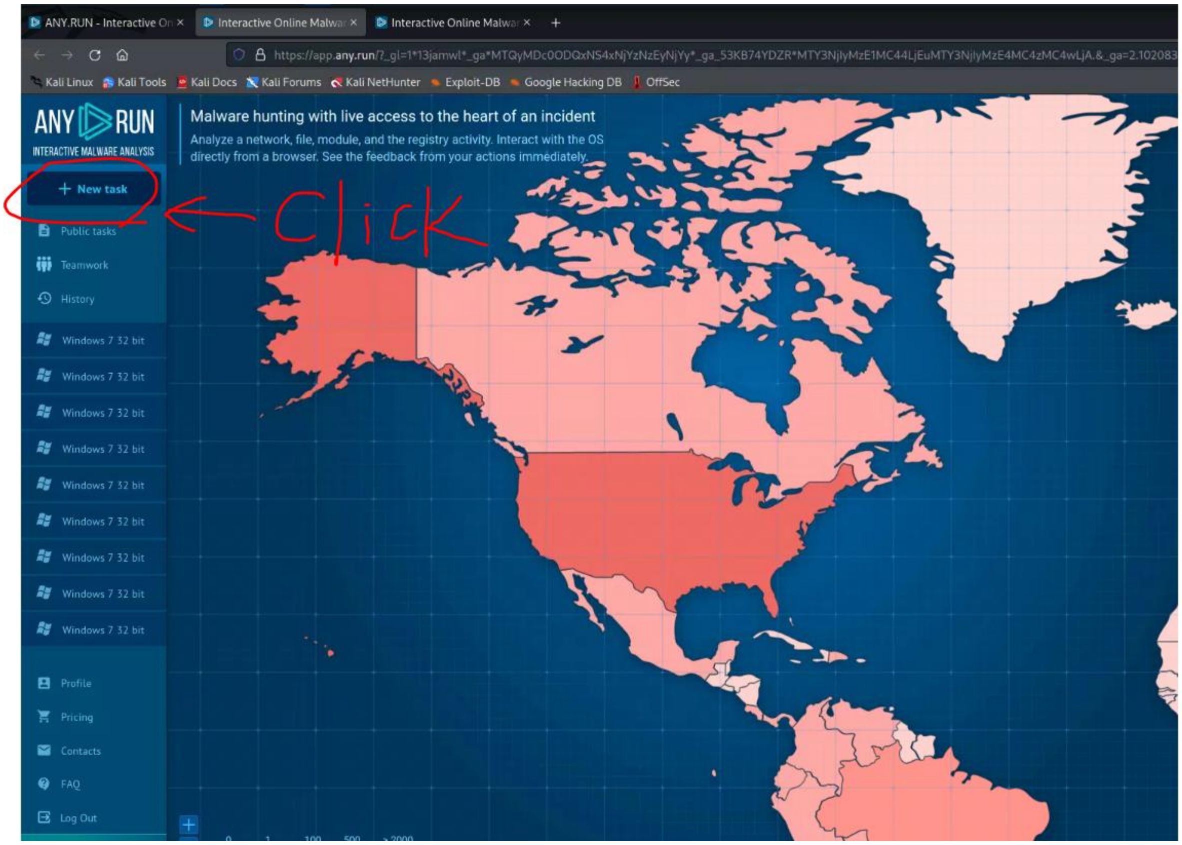
© 2023 GitHub, Inc.



Task 3: Detonating the downloaded WannaCry ransomware file on the Any-Run sandbox

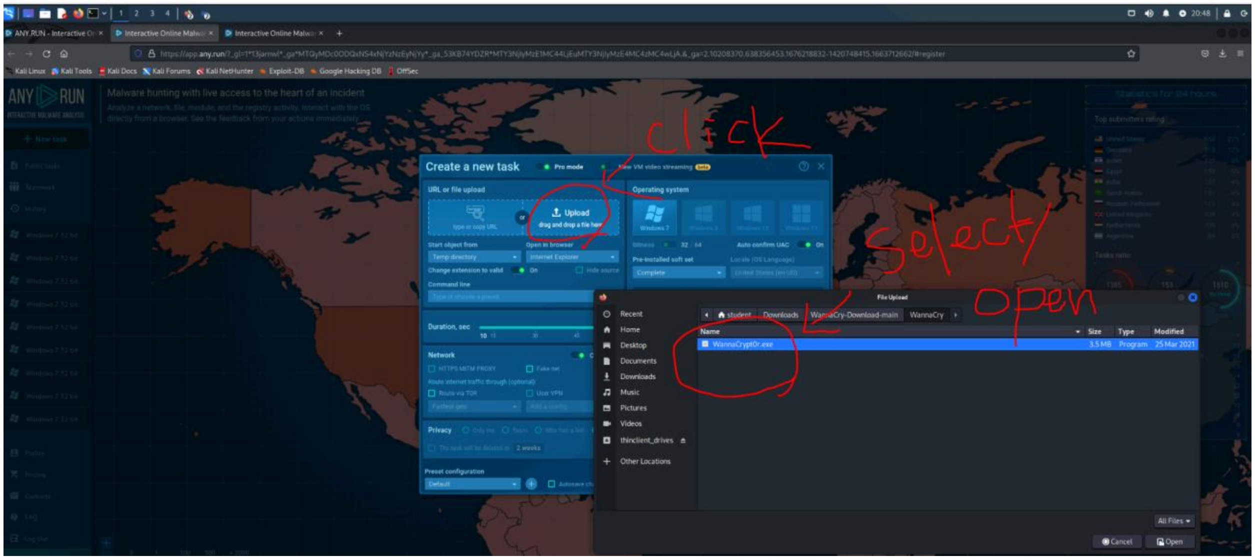
To detonate the downloaded ransomware file, you need to open the Any-Run sandbox, then upload the ransomware file Let's try this with step by step as the following:


https://any.run
WHY US
SERVICE
TRACKER
REPORTS
FEATURES
PRICING
BLOG
CONTACTS
MEDIA KIT
DEMO
MALWARE HUNTING WITH LIVE ACCESS TO THE HEART OF AN INCIDENT
Watch the epidemic as if it was on your computer, but in a more convenient and secure way, with a variety of monitoring features.
LET'S HUNT!
Click
REALTIME INTERACTION
NETWORK TRACKING

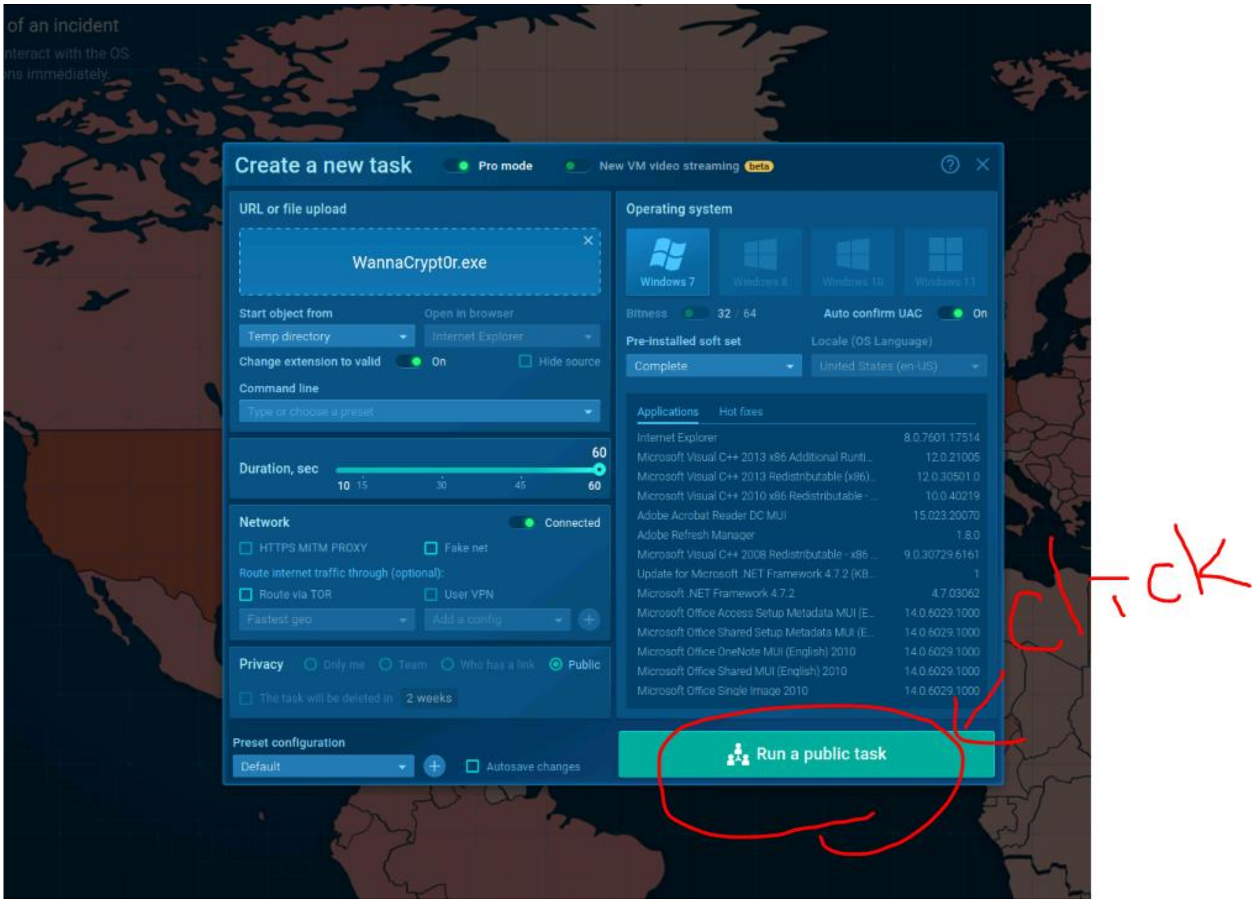


Malware hunting with live access to the heart of an incident

Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.



Lastly, click “Run as a public task” and detonate the ransomware.



of an incident
nteract with the OS
ns immediately

Create a new task ● Pro mode ● New VM video streaming beta

URL or file upload

WannaCrypt0r.exe

Start object from: Temp directory
Open in browser: Internet Explorer
Change extension to valid: ● On
□ Hide source
Command line: Type or choose a preset

Duration, sec: 60

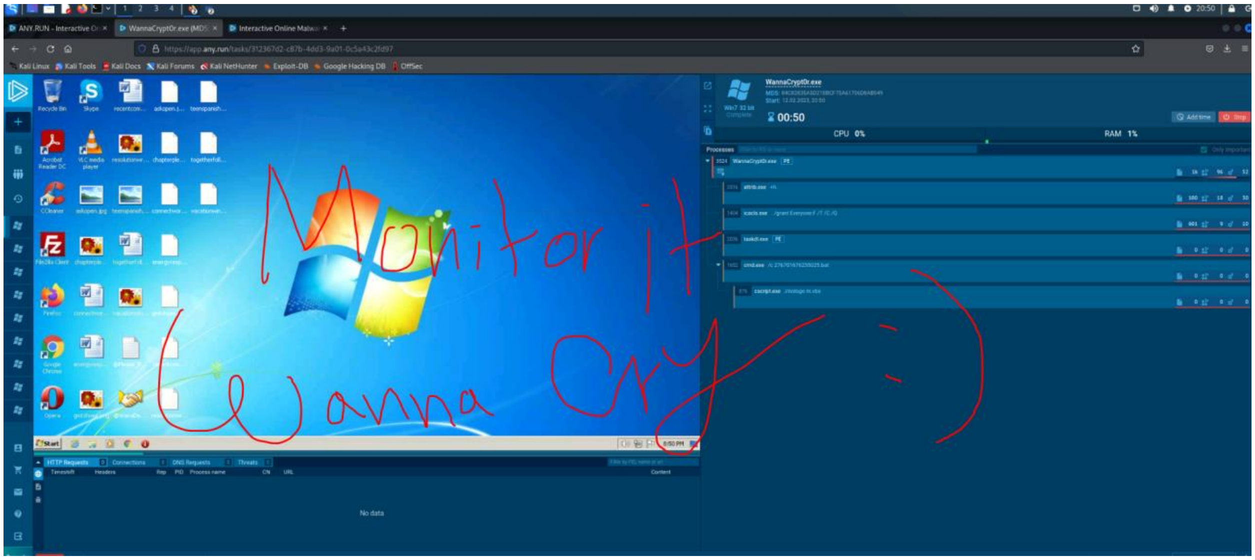
Network: ● Connected
□ HTTPS MITM PROXY
□ Fake net
Route internet traffic through (optional):
□ Route via TOR
□ User VPN
Fastest geo
Add a config

Privacy: ○ Only me ○ Team ○ Who has a link ● Public
□ The task will be deleted in 2 weeks

Preset configuration: Default
□ Autosave changes

Operating system: Windows 7 | Windows 8 | Windows 10 | Windows 11
Bitness: 32 / 64
Auto confirm UAC: ● On
Pre-installed soft set: Complete
Locale (OS Language): United States (en-US)

Applications	Hot fixes
Internet Explorer	8.0.7601.17514
Microsoft Visual C++ 2013 x86 Additional Runti...	12.0.21005
Microsoft Visual C++ 2013 Redistributable (x86)...	12.0.30501.0
Microsoft Visual C++ 2010 x86 Redistributable - ...	10.0.40219
Adobe Acrobat Reader DC MUI	15.023.20070
Adobe Refresh Manager	1.8.0
Microsoft Visual C++ 2008 Redistributable - x86 ...	9.0.30729.6161
Update for Microsoft .NET Framework 4.7.2 (KB...	1
Microsoft .NET Framework 4.7.2	4.7.03062
Microsoft Office Access Setup Metadata MUI (E...	14.0.6029.1000
Microsoft Office Shared Setup Metadata MUI (E...	14.0.6029.1000
Microsoft Office OneNote MUI (English) 2010	14.0.6029.1000
Microsoft Office Shared MUI (English) 2010	14.0.6029.1000
Microsoft Office Single Image 2010	14.0.6029.1000



https://app.any.run/tasks/312367d2-c87b-4dd3-9a01-0c5a43c2fd97

WannaCrypt0r.exe
MD5: 84C82835A5D21BBCF75A61706D8AB549
Start: 12.02.2023, 20:50
Win7 32 bit
Complete
00:50
CPU 0%
RAM 1%

```
Processes
3524 WannaCrypt0r.exe  PE
  2016 attrib.exe +h
  1404 icacls.exe ./grant Everyone:F /T /C /Q
  2036 taskdl.exe  PE
  1652 cmd.exe /c 276701676235025.bat
    876 cscript.exe //nologo m.vbs
```

No data

Enjoy WannaCry Ransomware!!!