**Nwachukwu Edumanichukwu**

**CYBR 440 - Incident Detection and Response  
Module 10 Lab – Malware Analysis**

In this tenth lab, we will examine an online dynamic analysis sandbox/engine called Any.Run. This tool is a malware sandbox that runs executables and other objects in a secure sandbox and provides reports on the things that executable or object does, and looks for indicators of malicious actions. We will first walk through how to use the tool, and then we will examine a previously run analysis of Trickbot. This lab does not use the Bellevue IS Lab desktops or Bellevue Bank and Trust analyst desktops.Run sections but will use them for the Sysinternals sections.

**You will be required to submit the following graded items as part of this lab:**

* Answer all questions listed in **BOLD**
* Provide screenshots when asked

Part I - Registering and Running Any.Run

In this first lab, we will register for an Any.Run account and then use a URL to run the Palo Alto Wildfire test executable in the Any.Run sandbox.

1. Start by opening your browser and navigating to <https://any.run>. Then, press the Let’s Hunt link/button to continue.

Graphical user interface, text

Description automatically generated

1. On the app.any.run/#register page, enter your name, email address, and password. You can use a throw-away account, or you can use a personal or your Bellevue account. You can continue to use this service for free after the course. Make sure you do not use a throw-away account if you want to continue to use the service. Answer the questions, click to acknowledge the terms of use, make sure you uncheck the Subscribe to our newsletter if you don’t want email SPAM, complete the CAPTCHA, then click register. You will receive a registration pop-up and an email to validate your email address. Make sure you validate your email address.

A picture containing text, businesscard, screenshot

Description automatically generated

Graphical user interface, application, email

Description automatically generated

1. Return from the Any.Run site and click + New task on the left side of the screen.

Graphical user interface, application, website

Description automatically generated

1. One the Create a new task dialog, click on the left where it says type or copy URL and paste the following URL into the dialog: <https://wildfire.paloaltonetworks.com/publicapi/test/pe>. Change the toggle to Download the file and start. Click Run a public task. Click I Agree. Wait for the task to run.

Graphical user interface, website

Description automatically generated

1. The executable will do very little as it is not malicious and just set up to test another sandbox type. However, we will look at a malicious executable in the next lab.

**Paste the URL of your any.run task below. It will be in the format** [**https://app.any.run/tasks/{GUID}**](https://app.any.run/tasks/%7bGUID%7d)**.**

https://app.any.run/tasks/e1de7c55-8954-4edd-9570-0bfe60fb7826

Part 2 - Examining Trickbot in Any.Run

In this second lab, we will look at well-known malware called TrickBot as it has been run in Any.Run and examine the valuable types of information provided by Any.Run.

1. Open the link <https://any.run/report/34d0f663295e00b520c7801a21ec8303a850e04bd075dc3a4eb5dca1a6bddfee/69cc3af3-4879-44a3-8500-b7ca2f62cf43>. Scroll through this page and look at the different information provided. Answer the following questions.

**What is the name of the original file run?**

**saryacan.bin**

**What are the MD5 and SHA256 hashes of the malicious file run?  
  
Md5: 380DC556F2C6FA232C0A7A5140F91201  
SHA256: 34D0F663295E00B520C7801A21EC8303A850E04BD075DC3A4EB5DCA1A6BDDFEE**

**What types of malicious behaviors were observed?  
  
Known privilege escalation attack**

* DllHost.exe (PID: 1584)

**Loads the Task Scheduler COM API**

* tasyacan.bin.exe (PID: 2592)
* tasyacan.bin.exe (PID: 1488)

**Connects to CnC server**

* tasyacan.bin.exe (PID: 1488)

**Changes settings of System certificates**

* tasyacan.bin.exe (PID: 1488)

**Trickbot detected**

* tasyacan.bin.exe (PID: 1488)

**What type of suspicious behaviors was observed?**

**Starts SC.EXE for service management**

cmd.exe (PID: 3716)

cmd.exe (PID: 1452)

cmd.exe (PID: 2564)

cmd.exe (PID: 2500)

**Executes PowerShell scripts**

cmd.exe (PID: 664)

cmd.exe (PID: 556)

**Starts CMD.EXE for commands execution**

saryacan.bin.exe (PID: 3372)

tasyacan.bin.exe (PID: 2592)

**Creates files in the user directory**

saryacan.bin.exe (PID: 3372)

tasyacan.bin.exe (PID: 1488)

**Executable content was dropped or overwritten**

saryacan.bin.exe (PID: 3372)

**Application launched itself**

saryacan.bin.exe (PID: 1348)

tasyacan.bin.exe (PID: 2536)

tasyacan.bin.exe (PID: 3904)

tasyacan.bin.exe (PID: 3492)

**Creates files in the Windows directory**

tasyacan.bin.exe (PID: 3904)

tasyacan.bin.exe (PID: 1488)

tasyacan.bin.exe (PID: 3492)

**Adds / modifies Windows certificates**

tasyacan.bin.exe (PID: 1488)

**Removes files from Windows directory**

tasyacan.bin.exe (PID: 3904)

tasyacan.bin.exe (PID: 1488)

tasyacan.bin.exe (PID: 3492)

**Connects to unusual port**

tasyacan.bin.exe (PID: 1488)

**What high-level static analysis tasks were performed?**

**TRiD:**

**.exe - Win32 Executable Microsoft Visual Basic 6 (84.4)**

**.dll - Win32 Dynamic Link Library (generic) (6.7)**

**.exe - Win32 Executable (generic) (4.6)**

**.exe - Generic Win/DOS Executable (2)**

**.exe - DOS Executable Generic (2)**

**EXIF:**

**EXE**

**OriginalFileName: HP\_Math.exe**

**InternalName: HP\_Math**

**ProductVersion: 1**

**FileVersion: 1**

**ProductName: HP\_Math**

**FileDescription: This little demonstrates the ability of VB to go beyond**

**CompanyName: NeoProgrammics**

**CharacterSet: Unicode**

**LanguageCode: English (U.S.)**

**FileSubtype: 0**

**ObjectFileType: Executable application**

**FileOS: Win32**

**FileFlags: (none)**

**FileFlagsMask: 0x0000**

**ProductVersionNumber: 1.0.0.0**

**FileVersionNumber: 1.0.0.0**

**Subsystem: Windows GUI**

**SubsystemVersion: 4**

**ImageVersion: 1**

**OSVersion: 4**

**EntryPoint: 0x1410**

**UninitializedDataSize: 0**

**InitializedDataSize: 352256**

**CodeSize: 28672**

**LinkerVersion: 6**

**PEType: PE32**

**TimeStamp: 2018:06:29 09:46:07+02:00**

**MachineType: Intel 386 or later, and compatibles**

**Paste a screenshot of the behavior graph belowDiagram

Description automatically generated**

**How many times did this malicious executable write to the Windows registry?**

**23**

**How many suspicious files were created or downloaded?**

**43**

**What URL was used to download an authrootstl.cab file? What was the hostname? Why is this suspicious?**

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab

**What two DNS requests were made?**

Api.ip.sb   
www.download.windowsupdate.com

1. Click on the full analysis link at the top of this report. The link is <https://app.any.run/tasks/69cc3af3-4879-44a3-8500-b7ca2f62cf43>.
2. Look at the right of the screen. Notice the Get Sample link. This link can be used to download the file ran, in a zip file with the password infected. Do not click this link.
3. Click the IOC Link.

What IOCs were automatically detected by Any.Run?

**Main object - saryacan.bin**

sha256 34d0f663295e00b520c7801a21ec8303a850e04bd075dc3a4eb5dca1a6bddfee

sha1 b1660a71e8f19ab2e009113a3a1ad3b6c503b463

md5 380dc556f2c6fa232c0a7a5140f91201

**Dropped executable file**

sha256 C:\Users\admin\AppData\Roaming\sysmon\tasyacan.bin.exe 34d0f663295e00b520c7801a21ec8303a850e04bd075dc3a4eb5dca1a6bddfee

**Connections**

ip 195.54.163.33

ip 37.230.116.35

ip 185.146.156.237

ip 47.52.62.55

1. Exit out of the IOC dialog then click Process graph. This shows every other process that was started by the original malicious executable.

**The name of the first executable was named saryacan.bin.exe. There is another executable that executes after the first. What is the name of this second executable?**

tasyacan.bin.exe

**What are some of the other system tools run by these executables? There are three.**

Powershell.exe, sc.exe, cmd.exe

1. Exit the Process graph view and click the Mitre ATT&CK Matrix link. Click on one of the techniques to view more detailed information.

**Which tactics were used in this attack?**Abuse Elevation Control Mechanism: Bypass User Account Control

**Which techniques were used in this attack?**Lateral Movement

Eventvwr.exe which can auto-elevate and execute a specified binary or script.

1. Close all technique windows and then close the ATT&CK matrix view. Look at the bottom of the screen. Examine the HTTP Request, Connections, DNS Requests, and Threats tabs. Download the PCAP file by clicking the PCAP link. On the Connections tab, you can see flags under the CN column. Hovering over these flags will give you the country name.

**Hosts from which three countries were used in this attack?**

Hong Kong, Russian Federation, Ukraine.

Accessing the Lab

This lab is hosted in the university IS Lab and requires special instructions to access it. If you are not familiar with accessing the IS Lab, please see the document in this course that walks you through accessing the Cybersecurity Desktop. You can access the Cybersecurity Desktop through the Web or using VMWare’s Horizon client. It would be best if you used the native Horizon client when possible as it provides better performance. The web client can be accessed at <https://workspace.bellevue.edu>. Make sure you log in to this interface with your Bellevue student ID and password.

After accessing workspace.bellevue.edu and selecting the IS Lab desktop, open a browser and navigate to <https://10.98.100.11>. The first time you access this site, you will see a warning in the browser. Make sure to click advanced and then Proceed to 10.98.100.11 (Unsafe). Next, you should see the following remote access page.

Graphical user interface, application, Word

Description automatically generated

After accessing Bellevue Bank and Trust’s Remote Management Portal, login in using the following information:

* Username: analyst# - Where # is the number provided to you by your instructor
* Password: An@lyst#!! - Where # is the number provided to you by your instructor

After logging in, you should see the following page:

Graphical user interface, application

Description automatically generated

You should have three available connections, RDP Kali #, RDP Workstation#, and SSH Kali #. These are the three analyst tools you will use throughout this course.

You will be using the Windows 10 RDP Workstation# connection for this lab. Therefore, it would be best to open each new RDP or SSH connection in a new tab.

Part 3 - Dynamic and Static Analysis with Sysinternals

In this lab, we look at Sysinternals Process Explorer, Process Monitor, and Autoruns to examine a system for malware.

1. Start by accessing your analyst workstation as described above. After gaining access to your analyst workstation, navigate on the desktop to the CYBR 440 folder then the SysinternalsSuite or C:\CYBR 440\SysinternalsSuite.
2. Double-click ProcExp64. Accept the license agreement, and the process explorer Window appears. Start by looking at the process explorer tree. This view display similar information to Task Manager but provides a lot more functionality. Notice that the different processes are highlighted in different colors. The meaning of the colors are as follow:
   1. The color purple in Process Explorer is an indication that the files may be packed.
   2. The color red means that the process is exiting (being stopped).
   3. The color green means the process was freshly spawned (just loaded).
   4. The light blue processes are those run by the same account that started Process Explorer.
   5. The dark blue indicates that the process is selected (by clicking or otherwise).
   6. The color pink indicates that the process is a service (like our friend svchost.exe).
   7. If you “Suspend” a process it will turn dark grey until you “Resume” it.

Table

Description automatically generated with medium confidence

1. Besides simply becoming familiar with Windows services and processes, there are a few quick ways to check for Malware with Process Explorer. First, we can check for unsigned programs executing. While there are ways around having malware execute as a cryptographically signed process (such as sideloading), this is an advanced technique that is not commonly used by most malware. Navigate to the menu Options -> Verify image signatures. Another column named Verified Signer will appear with the company's name that has signed the process/image. Unsigned images are an excellent place to start looking for suspicious processes.

**Which processes have not been signed?**

Microsoft Photos.exe

1. Now click Options -> VirusTotal.com -> Check VirusTotal.com. This adds another column that displays the number of anti-virus that see that process as malicious. Note, that you may have to run this process a few times by checking and unchecking VirusTotal.com as the direction Internet connection from the lab is sometimes spotty.

**Are there any processes detected as malicious by VirusTotal? Are there any other interesting results?**

All access is denied under the virus total and the Secure System, Registry and Memory Compression have the error message “The system cannot find the file specified”.

1. Close Process Explorer and open Autoruns64. Click Agree to accept the software license. Autoruns automatically scans the system for anything that is configured to start when Windows starts. Persistent malware must schedule itself to start on system startup, so this is another good place to look for malware. Notice that we have a publisher columns next to the things scheduled for startup. Autoruns verifies signatures for us automatically. Scroll through the list of startup items.

**Is anything unsigned (Not verified, if so what? What other issues do you see when looking at the Publisher column?**

**\Microsoft\\Windows\Autochk\Proxy --- File not found: /d.exe**

**\Microsoft\\Windows\HelloFace\FODCleanTask**

**\npcawatchdog**

**Nxlog, Ssh-agent, sshd, CimFS, ElasticELAMDriver**

**SysmonDrv --- File not found: SysmonDrv.sys**

**Adobe Type Manager --- File not found: atmfd.dll**

**\_wow64cpu --- File not found: C:\WINDOWS\Syswow64\wow64cpu.dll**

**\_wowarmhw --- File not found: C:\WINDOWS\System32\ wowarmhw.dll**

**\_wowarmhw --- File not found: C:\WINDOWS\ Syswow64\ wowarmhw.dll**

**\_xtajit --- File not found: C:\WINDOWS\System32\ xtajit.dll**

**\_xtajit --- File not found: C:\WINDOWS\ Syswow64\ xtajit.dll**

**\_wow64 --- File not found: C:\WINDOWS\ Syswow64\ wow64.dll**

**\_wow64win --- File not found: C:\WINDOWS\ Syswow64\ wow64win.dll**

1. Navigate to Options -> Scan Options. In the dialog that appears, select Check VirusTotal.com and click rescan. Click Yes to accept VirusTotals terms of service. Note that missing files will not be scanned for obvious reasons. Scanning of all files may not take place due to the lab's inconsistent Internet connection.
2. Close Autoruns and open ProcMon64 and agree to the software license. Notice that the processes listed in the process column has records for every registry, file, network, and device access for the process. This is an excellent tool to use when investigating everything malware does on a system. However, we will not delve further into this tool as it takes a while to learn and is more complex than the others.

**Take a screenshot of the main process monitor windows and paste it below.**

**A picture containing table

Description automatically generated**