CA-03

INT-301: Open Source and Technologies

Report of project

Name of Student: Drishti Singh

Registration no: 11905487

Roll no. 01

Git hub Link;

https:

Name of Faculty: Dr. Rajeshwar Sharma

Introduction:

Objective of the project:

To use any available Open-source Software to trace API calls and behavior of the files. Also, to analyze malicious files if available and prepare a detailed report on that. Then To start Unifi Network Controller or Network application to update and upgrade it automatically.

Description of the project:

To trace API calls and behavior of files, one popular open-source tool is Cuckoo. It provides deep visibility into Linux system behavior by capturing system calls, network activity, and other system events. Cuckoo can generate detailed reports on system activity and provide real-time analysis of system events.

To analyze malicious files, ClamAV is a widely used open-source antivirus tool. It can scan files for viruses, malware, and other malicious content. ClamAV can be configured to scan files automatically in real-time or on-demand.

To start UniFi Network Controller and upgrade/update automatically, Ansible is a popular open-source tool for automation. Ansible can be used to automate the deployment of UniFi Network Controller and to perform upgrades and updates automatically.

To create an HTML report of system activity, we can use the Elasticsearch-Logstash-Kibana (ELK) stack. Logstash can be used to collect and parse system logs, which can then be indexed in Elasticsearch. Kibana can then be used to generate visualizations and reports based on the indexed data.

To create favorites for instant access to hardware components from the menu bar, we can use the GNOME desktop environment on Linux. GNOME provides a customizable favorites menu that can be populated with shortcuts to frequently used applications and files.

Overall, by using these open-source tools, we can achieve comprehensive system monitoring, antivirus protection, and automation for the UniFi Network Controller.

Scope of the project:

Cuckoo is an open-source software that can be used for automated malware analysis. It is designed to detect malware by analyzing its behavior rather than relying on signature-based detection methods.

When a suspicious file is uploaded to Cuckoo, it runs the file in a virtual environment and monitors its behavior, such as file system changes, network activity, and system calls. It then generates a report of the analysis, including any malicious actions or indicators of compromise that were detected.

Cuckoo can be useful for several purposes, such as:

Malware detection: Cuckoo can detect previously unknown malware by analyzing its behavior and identifying malicious actions.

Malware analysis: Cuckoo can be used to analyze the behavior of malware to understand how it works and how it can be detected or mitigated.

Threat intelligence: Cuckoo can generate reports on the behavior of different types of malwares, which can be used to inform threat intelligence and help organizations better protect themselves against cyber-attacks.

Overall, Cuckoo is a powerful tool for automated malware analysis that can help security professionals detect and respond to cyber threats more effectively.

System Description:

Target system Description:

In computer security, a cuckoo is a type of malware analysis system that detects and analyzes malware by executing it in a virtual environment. The system is named after the cuckoo bird, which lays its eggs in other birds' nests and leaves the work of raising its offspring to the host bird.

A cuckoo system typically consists of a virtual machine (VM) that runs a target operating system (OS), a malware analysis tool, and a network monitoring component. When a suspicious file is detected, the cuckoo system executes it in the virtual environment and monitors its behavior for malicious activities such as network connections, file modifications, and system changes.

The target OS running in the VM is typically a lightweight version of Windows or Linux and is often configured with specific tools and settings to aid in malware analysis. The malware analysis tool used by cuckoo systems can vary, but typically includes signature-based scanners, behavioral analysis tools, and sandboxing mechanisms to isolate the malware from the host system.

The network monitoring component of cuckoo systems captures network traffic generated by the malware during its execution, allowing analysts to identify any communication with command-and-control servers, exfiltration of sensitive data, or other malicious activities.

The output of a cuckoo analysis typically includes a report that summarizes the malware's behavior, indicators of compromise (IOCs), and recommendations for remediation. This information is used by security analysts to identify and mitigate threats, and to improve the overall security posture of an organization.

Assumptions and Dependencies:

assume that you are referring to the Cuckoo hashing algorithm, which is a data structure used for hash table implementations.
Software requirements
python libraries
virtualization software
tcpdump
Volatility

Assumptions:

Uniform hashing: Cuckoo hashing assumes that the hash function used to map keys to indices in the hash table is uniformly distributed. That is, each key has an equal probability of being mapped to any slot in the hash table.

No duplicate keys: Cuckoo hashing assumes that there are no duplicate keys in the hash table. If there are, the algorithm may enter an infinite loop trying to find an empty slot for the key.

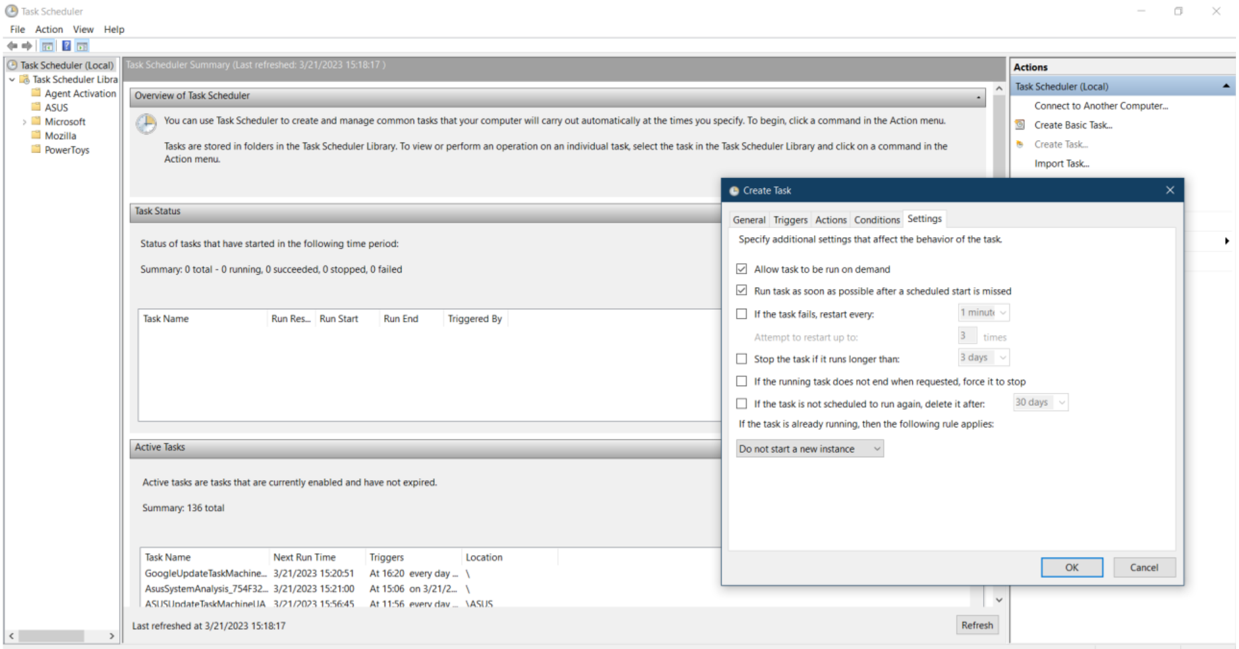
Dependencies:

Hash function: Cuckoo hashing depends on a hash function to map keys to indices in the hash table. The quality of the hash function can affect the performance of the algorithm, as a poor hash function may result in many collisions and longer lookup times.

Number of hash tables: Cuckoo hashing uses multiple hash tables to store keys, and the number of hash tables used affects the performance of the algorithm. Increasing the number of hash tables can reduce the likelihood of collisions, but also increases the space overhead of the data structure.

Load factor: The load factor of the hash table, which is the ratio of the number of keys to the number of slots in the hash table, can also affect the performance of the algorithm. Higher load factors can increase the likelihood of collisions and longer lookup times, while lower load factors can result in wasted space in the hash table.

Analysis Report: Figure 1.1



Task Scheduler

File Action View Help

Task Scheduler (Local)
Task Scheduler Libra
Agent Activation
ASUS
Microsoft
Mozilla
PowerToys

Task Scheduler Summary (Last refreshed: 3/21/2023 15:18:17)

Overview of Task Scheduler

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Task Status

Status of tasks that have started in the following time period:

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

Task Name	Run Res...	Run Start	Run End	Triggered By

Active Tasks

Active tasks are tasks that are currently enabled and have not expired.

Summary: 136 total

Task Name	Next Run Time	Triggers	Location
GoogleUpdateTaskMachine...	3/21/2023 15:20:51	At 16:20 every day ...	\
AsusSystemAnalysis_754F32...	3/21/2023 15:21:00	At 15:06 on 3/21/2...	\
ASUSUpdateTaskMachineUA	3/21/2023 15:56:45	At 11:56 every day ...	\ASUS

Last refreshed at 3/21/2023 15:18:17

Refresh

Actions

Task Scheduler (Local)

Connect to Another Computer...

Create Basic Task...

Create Task...

Import Task...

Create Task

General Triggers Actions Conditions Settings

Specify additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☑ Run task as soon as possible after a scheduled start is missed

□ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

□ Stop the task if it runs longer than: 3 days

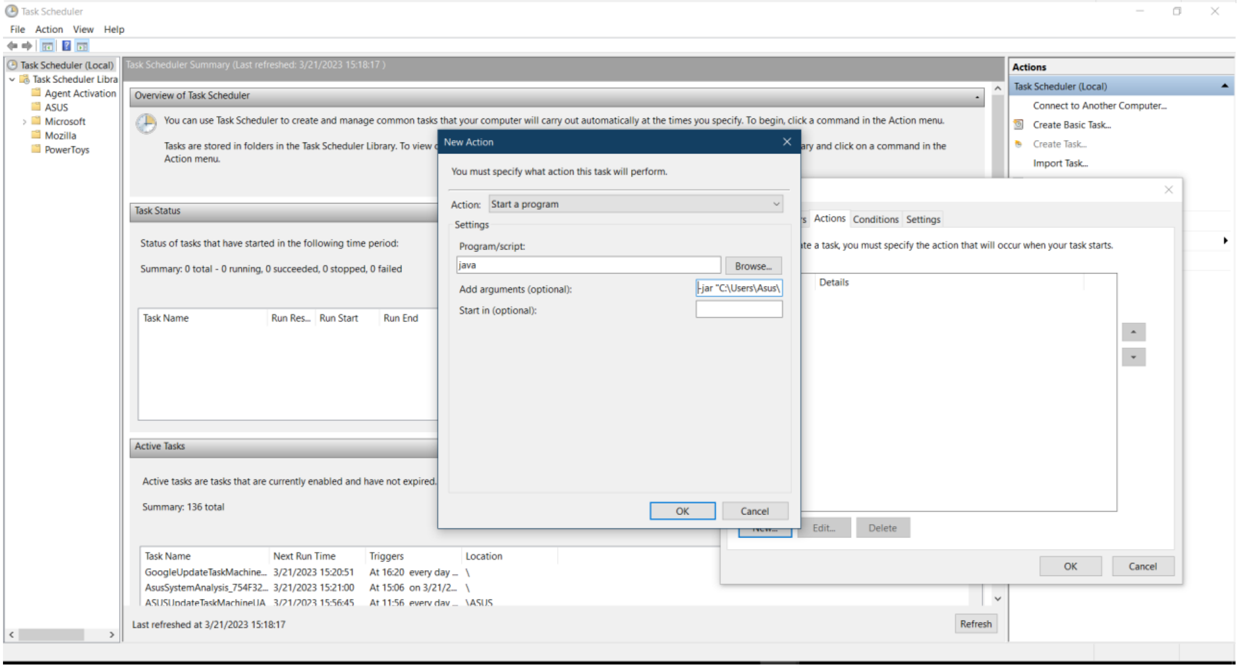
□ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

OK Cancel



Task Scheduler

File Action View Help

Task Scheduler (Local)
Task Scheduler Libra
Agent Activation
ASUS
Microsoft
Mozilla
PowerToys

Task Scheduler Summary (Last refreshed: 3/21/2023 15:18:17)

Overview of Task Scheduler

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view o ary and click on a command in the Action menu.

Task Status

Status of tasks that have started in the following time period:

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

Task Name	Run Res...	Run Start	Run End

Active Tasks

Active tasks are tasks that are currently enabled and have not expired.

Summary: 136 total

Task Name	Next Run Time	Triggers	Location
GoogleUpdateTaskMachine...	3/21/2023 15:20:51	At 16:20 every day ...	\
AsusSystemAnalysis_754F32...	3/21/2023 15:21:00	At 15:06 on 3/21/2...	\
ASUSUpdateTaskMachineUA	3/21/2023 15:56:45	At 11:56 every day ...	\ASUS

Last refreshed at 3/21/2023 15:18:17

Refresh

Actions

Task Scheduler (Local)

Connect to Another Computer...

Create Basic Task...

Create Task...

Import Task...

s Actions Conditions Settings

te a task, you must specify the action that will occur when your task starts.

Details

New... Edit... Delete

OK Cancel

New Action

You must specify what action this task will perform.

Action: Start a program

Settings

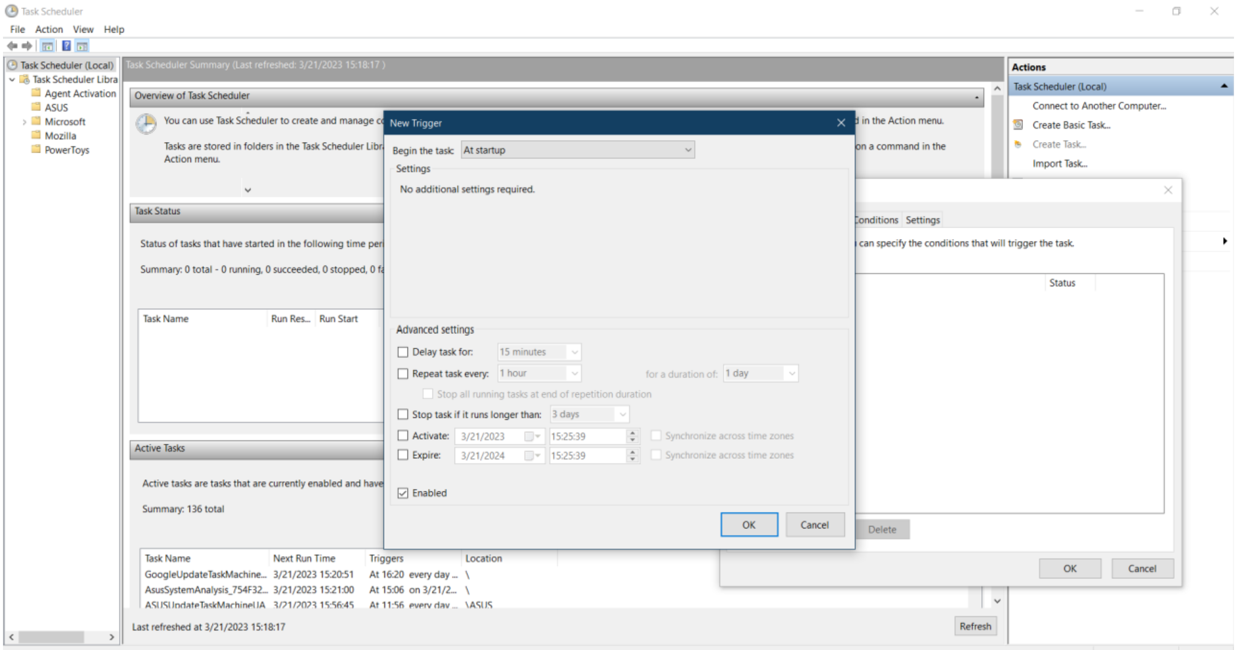
Program/script: java

Browse...

Add arguments (optional): -jar "C:\Users\Asus\

Start in (optional):

OK Cancel



Task Scheduler Summary (Last refreshed: 3/21/2023 15:18:17)

Overview of Task Scheduler

You can use Task Scheduler to create and manage c… in the Action menu.

Tasks are stored in folders in the Task Scheduler Libr… on a command in the Action menu.

Task Status

Status of tasks that have started in the following time per…

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 fa…

Task Name | Run Res... | Run Start

Active Tasks

Active tasks are tasks that are currently enabled and have…

Summary: 136 total

Task Name	Next Run Time	Triggers	Location
GoogleUpdateTaskMachine...	3/21/2023 15:20:51	At 16:20 every day ...	\
AsusSystemAnalysis_754F32...	3/21/2023 15:21:00	At 15:06 on 3/21/2...	\
ASUSUpdateTaskMachineUA	3/21/2023 15:56:45	At 11:56 every day ...	\ASUS

Last refreshed at 3/21/2023 15:18:17

…can specify the conditions that will trigger the task.

New Trigger

Begin the task: At startup

Settings

No additional settings required.

Advanced settings

☐ Delay task for: 15 minutes

☐ Repeat task every: 1 hour   for a duration of: 1 day

☐ Stop all running tasks at end of repetition duration

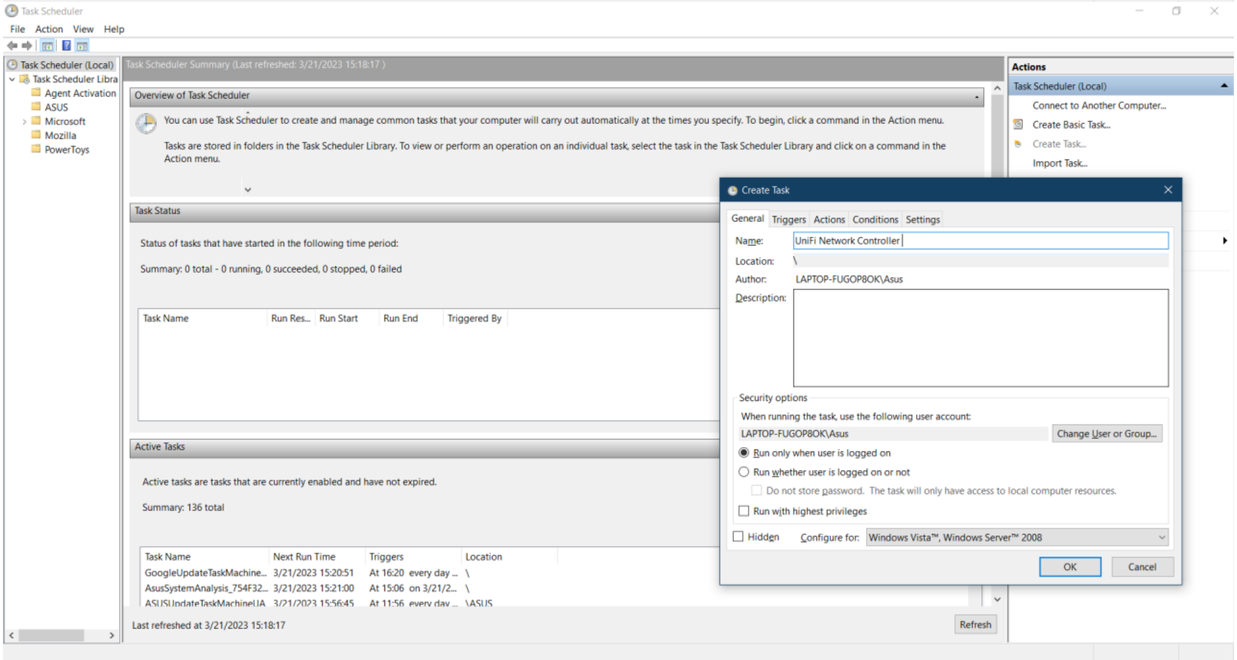
☐ Stop task if it runs longer than: 3 days

☐ Activate: 3/21/2023 15:25:39 ☐ Synchronize across time zones

☐ Expire: 3/21/2024 15:25:39 ☐ Synchronize across time zones

☑ Enabled

OK Cancel



Task Scheduler Summary (Last refreshed: 3/21/2023 15:18:17)

Overview of Task Scheduler

You can use Task Scheduler to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

Tasks are stored in folders in the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the Action menu.

Task Status

Status of tasks that have started in the following time period:

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

Task Name | Run Res... | Run Start | Run End | Triggered By

Active Tasks

Active tasks are tasks that are currently enabled and have not expired.

Summary: 136 total

Task Name	Next Run Time	Triggers	Location
GoogleUpdateTaskMachine...	3/21/2023 15:20:51	At 16:20 every day ...	\
AsusSystemAnalysis_754F32...	3/21/2023 15:21:00	At 15:06 on 3/21/2...	\
ASUSUpdateTaskMachineUA	3/21/2023 15:56:45	At 11:56 every day ...	\ASUS

Last refreshed at 3/21/2023 15:18:17

Create Task

General | Triggers | Actions | Conditions | Settings

Name: UniFi Network Controller

Location: \

Author: LAPTOP-FUGOP8OK\Asus

Description:

Security options

When running the task, use the following user account:

LAPTOP-FUGOP8OK\Asus   Change User or Group...

● Run only when user is logged on

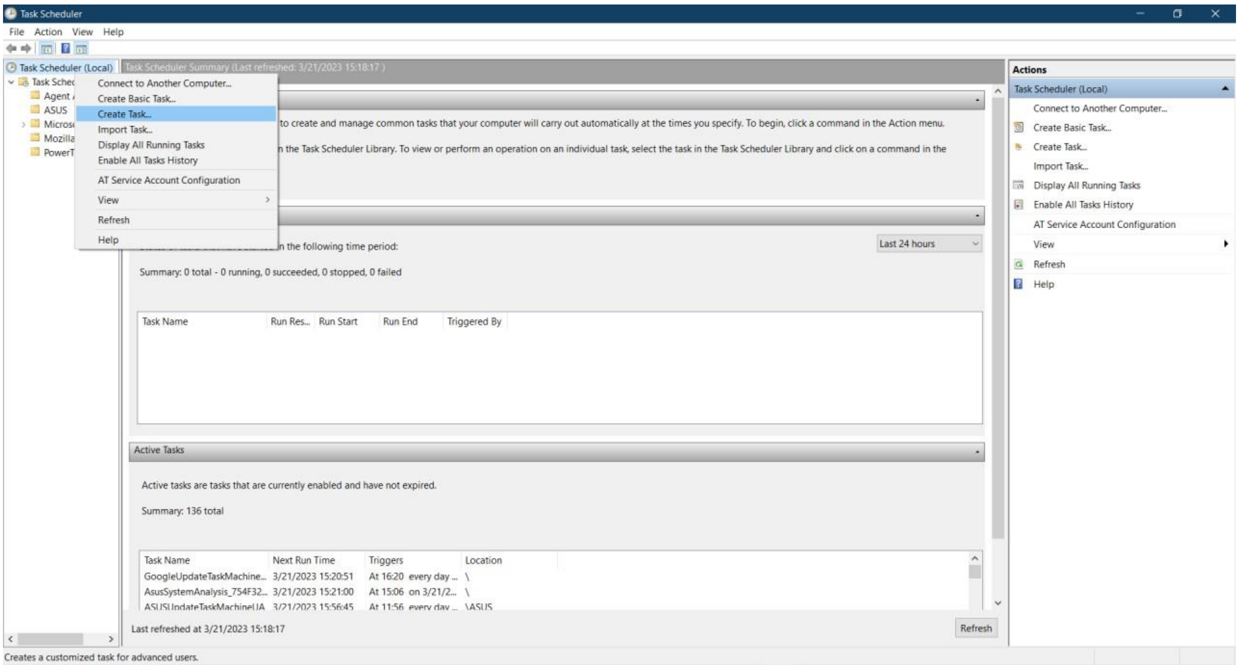
○ Run whether user is logged on or not

☐ Do not store password. The task will only have access to local computer resources.

☐ Run with highest privileges

☐ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

OK Cancel



to create and manage common tasks that your computer will carry out automatically at the times you specify. To begin, click a command in the Action menu.

n the Task Scheduler Library. To view or perform an operation on an individual task, select the task in the Task Scheduler Library and click on a command in the

n the following time period:

Summary: 0 total - 0 running, 0 succeeded, 0 stopped, 0 failed

Task Name	Run Res...	Run Start	Run End	Triggered By

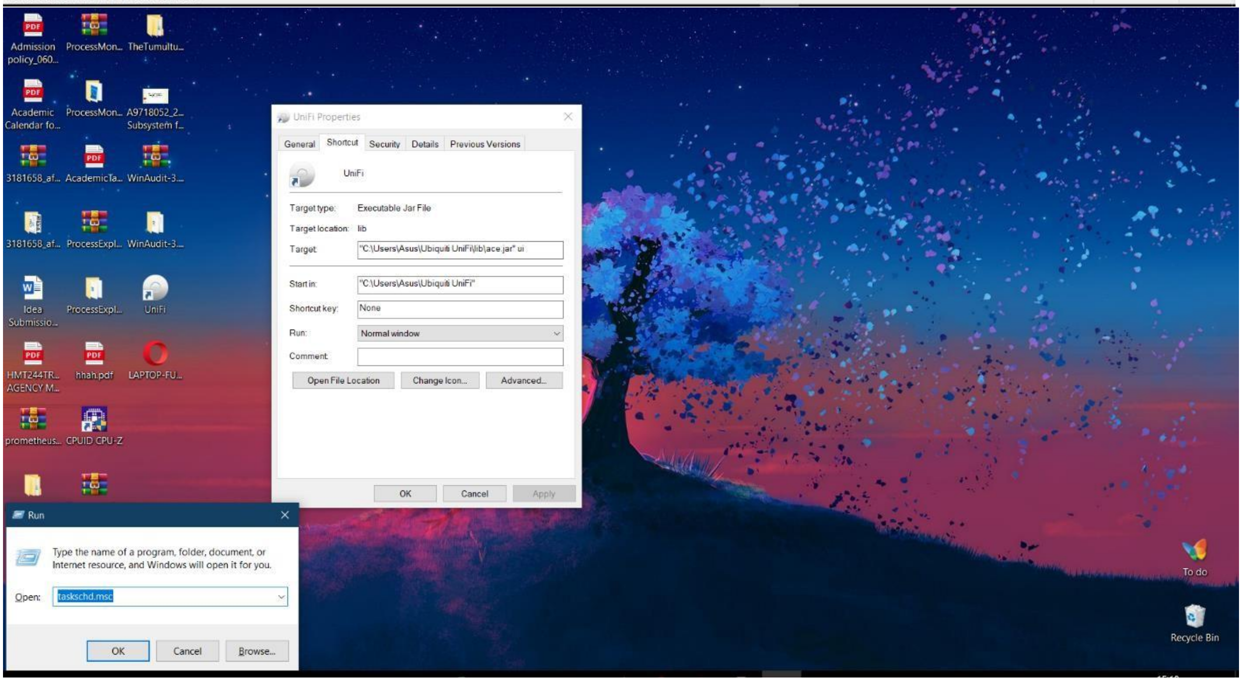
Active tasks are tasks that are currently enabled and have not expired.

Summary: 136 total

Task Name	Next Run Time	Triggers	Location
GoogleUpdateTaskMachine...	3/21/2023 15:20:51	At 16:20 every day ...	\
AsusSystemAnalysis_754F32...	3/21/2023 15:21:00	At 15:06 on 3/21/2...	\
ASUSUpdateTaskMachineUA	3/21/2023 15:56:45	At 11:56 every day ...	\ASUS

Last refreshed at 3/21/2023 15:18:17

Creates a customized task for advanced users.



Target type: Executable Jar File

Target location: lib

Target: "C:\Users\Asus\Ubiquiti UniFi\lib\ace.jar" ui

Start in: "C:\Users\Asus\Ubiquiti UniFi"

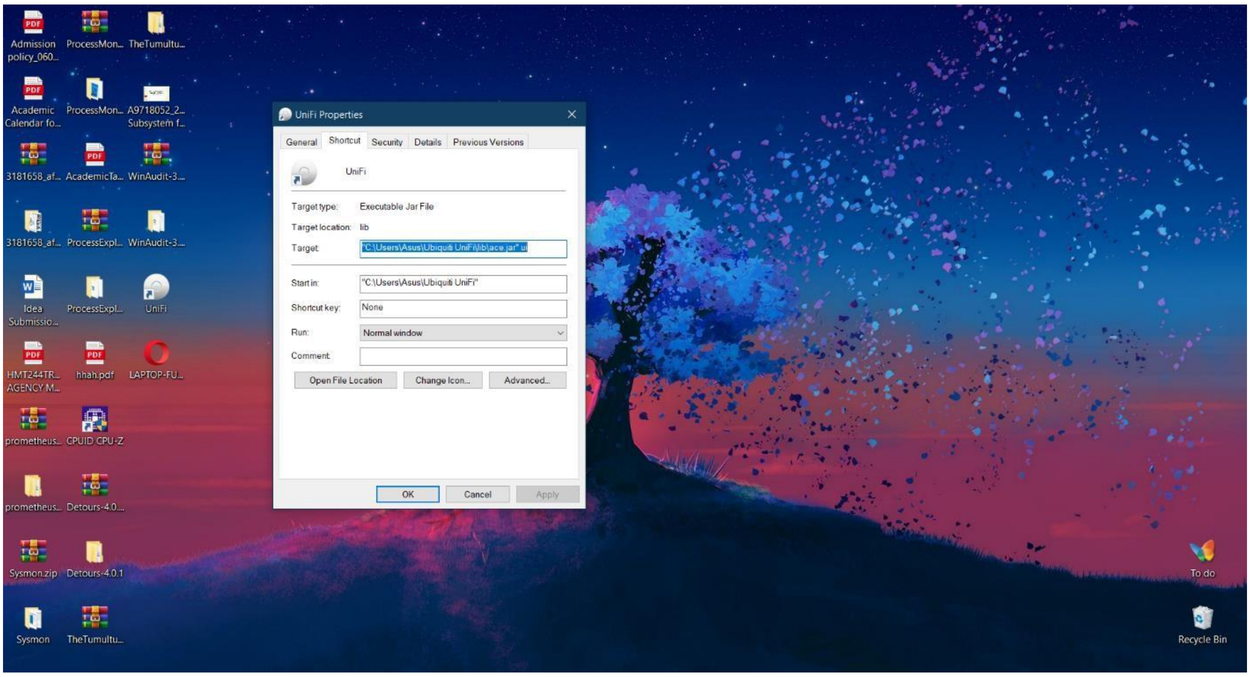
Shortcut key: None

Run: Normal window

Comment:

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: taskschd.msc



UniFi Properties

UniFi

Target type: Executable Jar File

Target location: lib

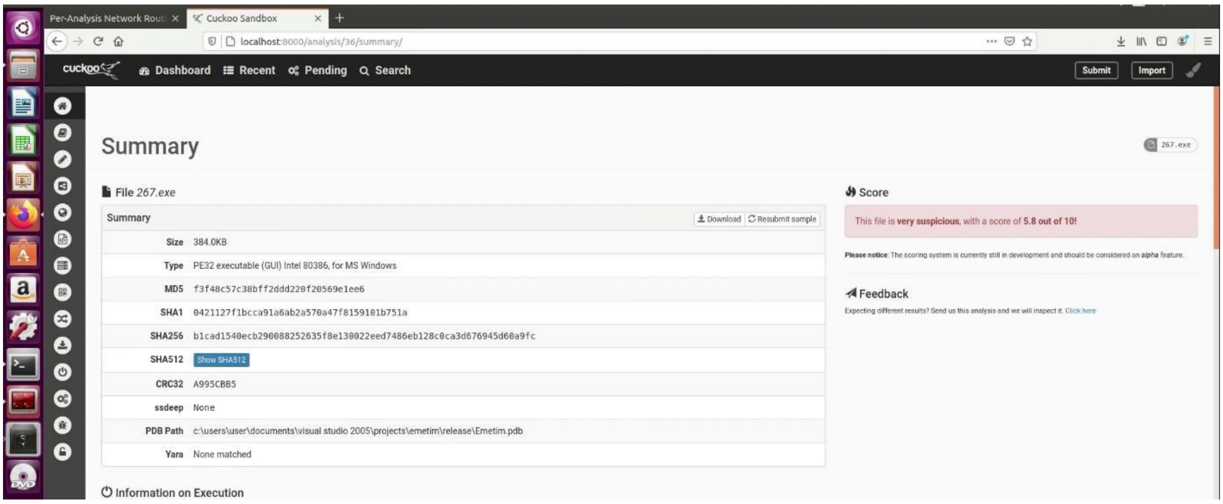
Target: "C:\Users\Asus\Ubiquiti UniFi\lib\ace.jar" ui

Start in: "C:\Users\Asus\Ubiquiti UniFi"

Shortcut key: None

Run: Normal window

Comment:



Summary

File *267.exe*

Summary

Size	384.0KB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	f3f48c57c38bff2ddd220f20569e1ee6
SHA1	0421127f1bcca91a6ab2a570a47f8159101b751a
SHA256	b1cad1540ecb290088252635f8e130022eed7486eb128c0ca3d676945d60a9fc
SHA512	Show SHA512
CRC32	A995CBB5
ssdeep	None
PDB Path	c:\users\user\documents\visual studio 2005\projects\emetim\release\Emetim.pdb
Yara	None matched

Score

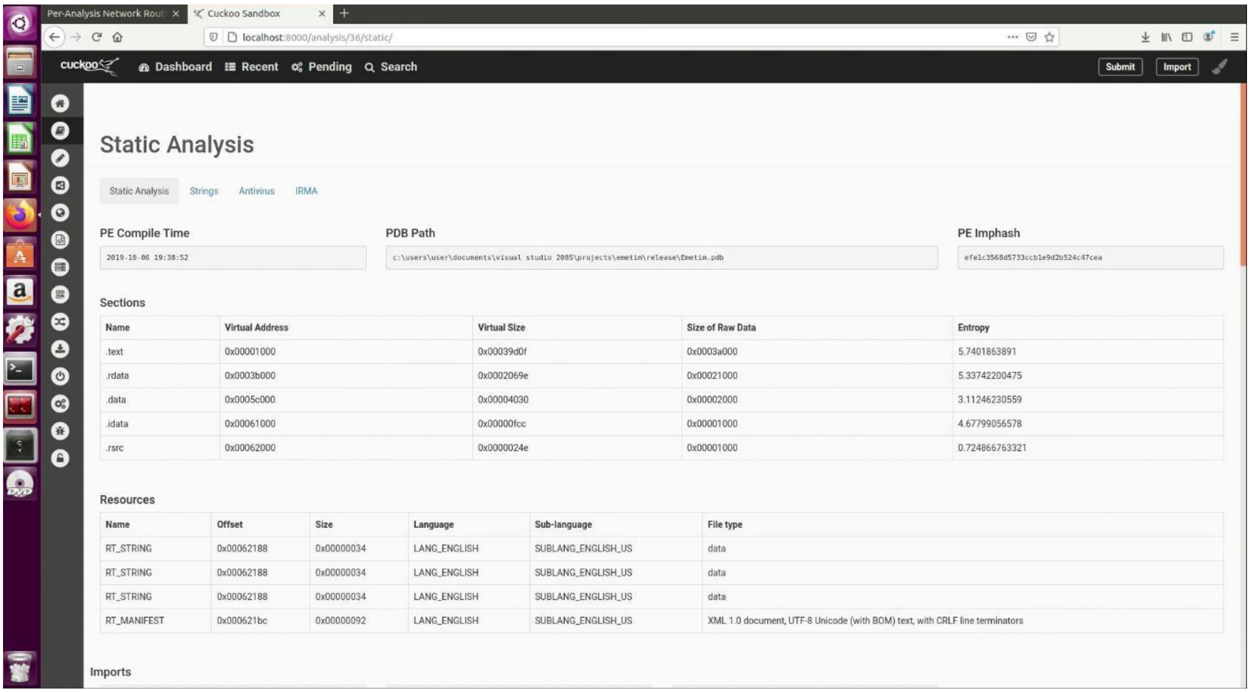
This file is **very suspicious**, with a score of **5.8 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an ***alpha*** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

Information on Execution



Static Analysis

Static Analysis | Strings | Antivirus | IRMA

PE Compile Time

2019-10-06 19:38:52

PDB Path

c:\users\user\documents\visual studio 2005\projects\emetim\release\Emetim.pdb

PE Imphash

efe1c3568d5733ccb1e9d2b524c47cea

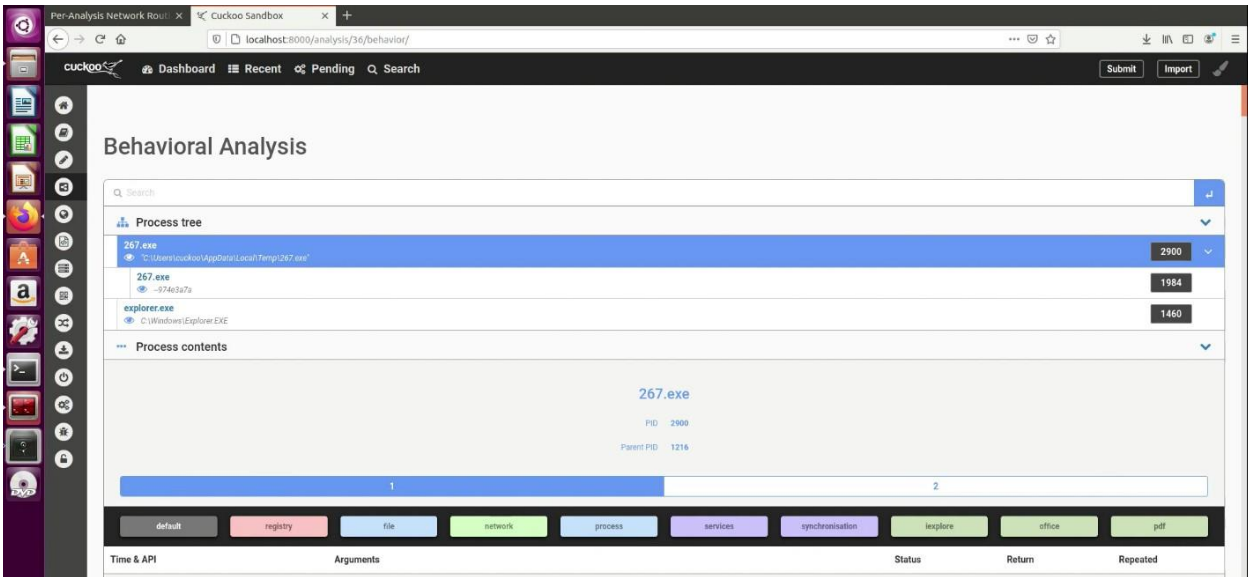
Sections

Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
.text	0x00001000	0x00039d0f	0x0003a000	5.7401863891
.rdata	0x0003b000	0x0002069e	0x00021000	5.33742200475
.data	0x0005c000	0x00004030	0x00002000	3.11246230559
.idata	0x00061000	0x00000fcc	0x00001000	4.67799056578
.rsrc	0x00062000	0x0000024e	0x00001000	0.724866763321

Resources

Name	Offset	Size	Language	Sub-language	File type
RT_STRING	0x00062188	0x00000034	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_STRING	0x00062188	0x00000034	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_STRING	0x00062188	0x00000034	LANG_ENGLISH	SUBLANG_ENGLISH_US	data
RT_MANIFEST	0x000621bc	0x00000092	LANG_ENGLISH	SUBLANG_ENGLISH_US	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators

Imports



Behavioral Analysis

Process tree

Process	PID
267.exe "C:\Users\cuckoo\AppData\Local\Temp\267.exe"	2900
267.exe -974e3a7a	1984
explorer.exe C:\Windows\Explorer.EXE	1460

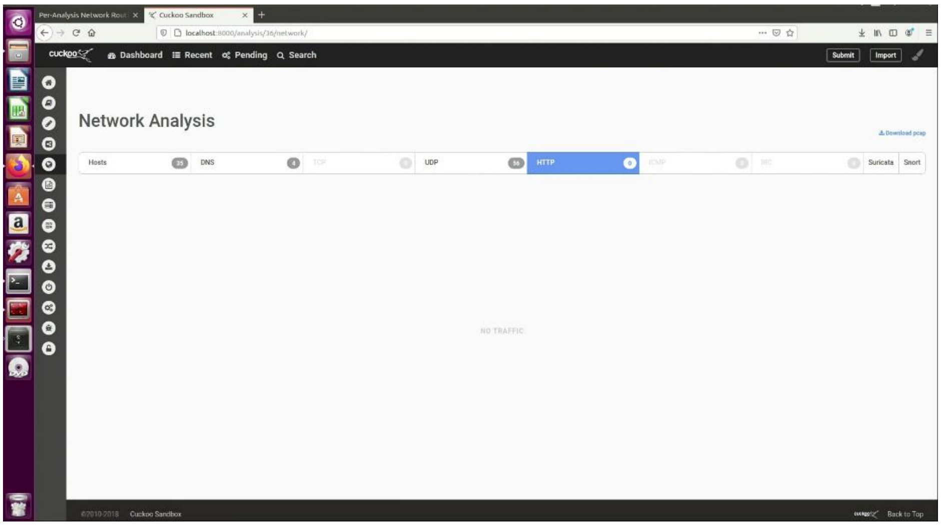
Process contents

267.exe

PID 2900

Parent PID 1216

Time & API	Arguments	Status	Return	Repeated



Network Analysis

Hosts	DNS	TCP	UDP	HTTP	ICMP	IRC	Suricata	Snort
35	4	0	56	0	0	0		

NO TRAFFIC

GIT HUB SCREENSHOTS: