Threat Categorization Based on Malware’s C2 Communication

Group 6 – (KCST) Kerberos Cyber Security Team

Date: 16th April 2023

Segments

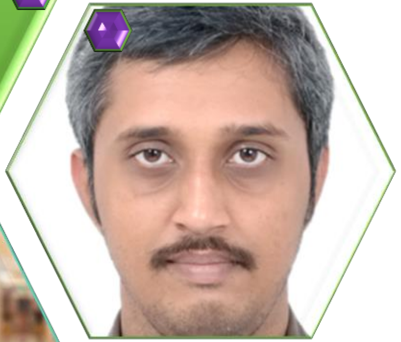
- TEAM
- PROBLEM STATEMENT
- PUT YOUR BEST WORK ON DISPLAY
- PICTURE ABHI BAKI HAI MERE DOST
- THE BEST IS YET TO COME
- ~~INTERROGATION~~ (Q&A)

Team

(Mentor)

Prof. Anand Handa

SRIRAM P



(Contributor)
Sec. Research Manager,
MacAfee

(Contributor)
DevOps Leader, IAEA

MOHAMMED JAWED

Mr. Nitesh Kumar

(Mentor)

ArkThor

Segment

TEAM

PICTURE ABHI BAKI HAI MERE DOST

PROBLEM STATEMENT

THE BEST IS YET TO COME

PUT YOUR BEST WORK ON DISPLAY

~~INTERROGATION~~ (Q&A)

Problem Statement

The threat landscape facing modern organizations is constantly evolving and becoming increasingly complex. With policies like BYOD and social data of individuals available on the social media, Passwords and 2FA are not going to stop the cyber attacks. Understanding the threat discovered in a corporate environment will help the infosec team to assess the impact of the attack and take measures accordingly Cyber-attacks are becoming more sophisticated and complex, and it is becoming increasingly difficult to detect and block /prevent them.

One of the key challenges in effectively defending against cyber threats is the ability to accurately categorize and analyze potential threats.

In particular, understanding the Command and Control (C2) communications used by attackers is critical in identifying and responding to cyber attacks. Command-and-Control (C2) communication is a common technique used by attackers to control the infected hosts and steal sensitive information. It is crucial to identify C2 communication and categorize the network threats accurately to prevent and mitigate cyber-attacks.

This project aims at looking into the networking concept of these C2 communicating malwares and tries to parse the network packets and classify the threats based on the unique communication pattern used by these malware families.

The rules also involve fingerprinting the TLS certificates used in the communication.

Segment

TEAM

PROBLEM STATEMENT

PUT YOUR BEST WORK ON DISPLAY

PICTURE ABHI BAKI HAI MERE DOST

THE BEST IS YET TO COME

~~INTERROGATION~~ (Q&A)

Capstone Project Introducing …

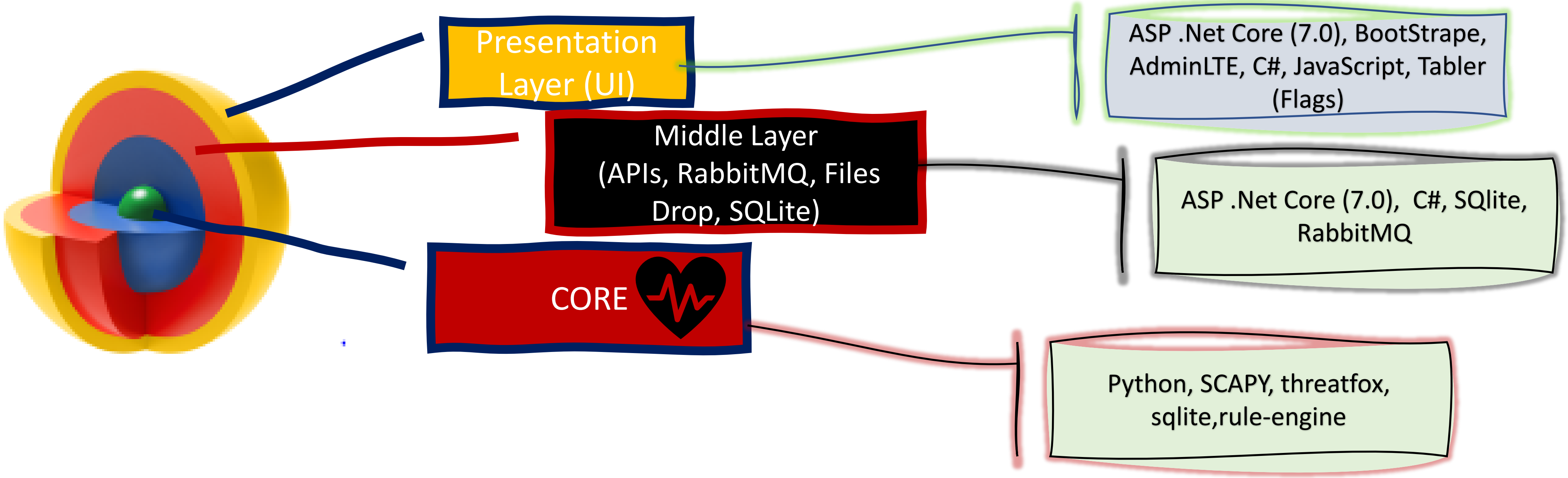
"As a result of this capstone project, we are proud to introduce **ArkThor**."

- **"Ark"** imply **safety** or **protection**
- **"Thor"** is associated with **strength** or **power**

"We aim to develop our capstone project into a fully functional product that can be brought to market and provide value to customers, rather than simply being a project for academic purposes."

Project Core Idea

- "The entire project is comprised of three distinct layers: a platform-independent layer that is scalable and built using microservices. It is also designed to be easy to deploy and relies entirely on an open-source technology stack.“
- "The inner layer can be used directly, without any dependencies on the upper layer."



Presentation Layer (UI)

ASP .Net Core (7.0), BootStrape, AdminLTE, C#, JavaScript, Tabler (Flags)

Middle Layer (APIs, RabbitMQ, Files Drop, SQLite)

ASP .Net Core (7.0), C#, SQlite, RabbitMQ

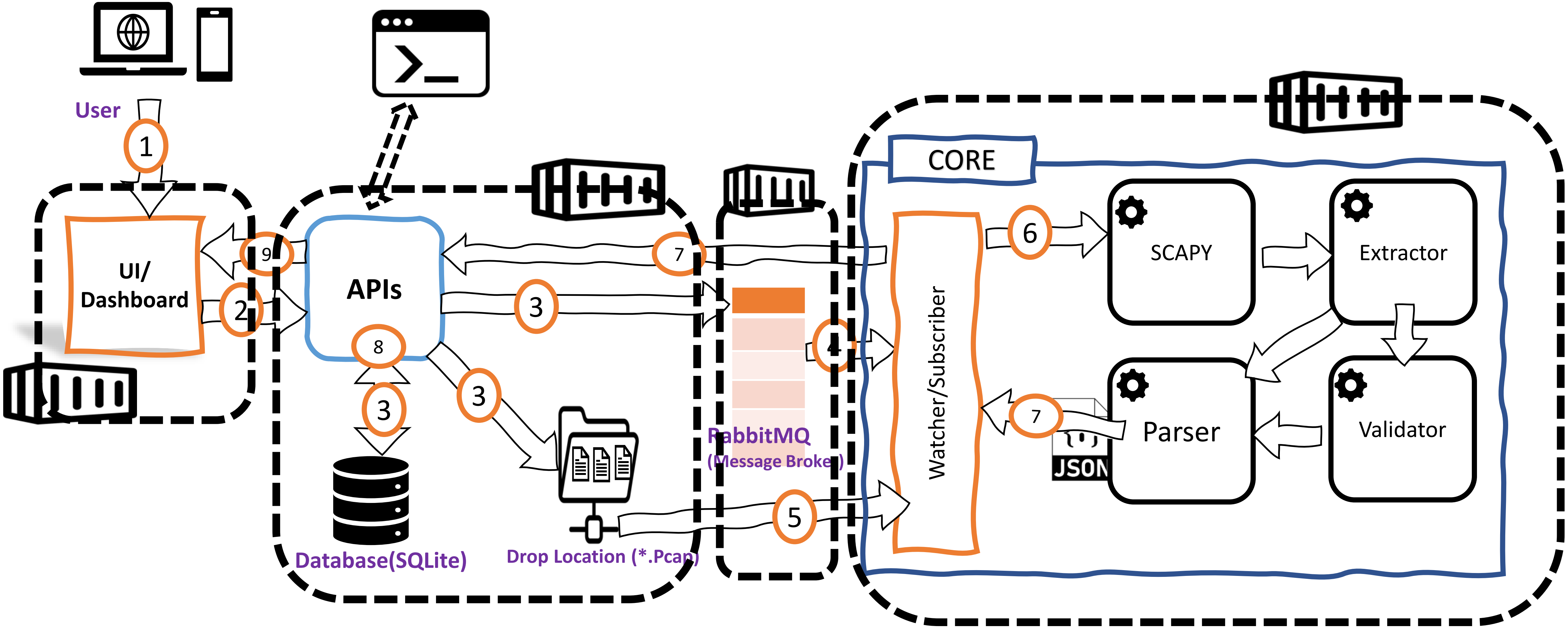
CORE

Python, SCAPY, threatfox, sqlite,rule-engine

Organization Don’t buy products, they buy Solution to their Problems….

ArkThor

ArkThor Connecting Dots ....



ArkThor

Front Engine Demo

Core Engine Demo

Segment

TEAM

PROBLEM STATEMENT

PUT YOUR BEST WORK ON DISPLAY

PICTURE ABHI BAKI HAI MERE DOST

THE BEST IS YET TO COME

~~INTERROGATION~~ (Q&A)

ArkThor to Grow Organically

"After consulting with our mentor and gaining approval to allow organic growth, we have made this project available on GitHub a open source project for people to contribute.

In addition, a public version can be viewed as the ArkThor sample on Azure Cloud."

1. GitHub repo Url
https://github.com/JawedCIA/ArkThor

2. Public Version
https://arkthor.azurewebsites.net/

ArkThor

Segment

TEAM

PROBLEM STATEMENT

PUT YOUR BEST WORK ON DISPLAY

PICTURE ABHI BAKI HAI MERE DOST

THE BEST IS YET TO COME

~~INTERROGATION~~ (Q&A)

Things to look forward

CORE

- Live Dump of Wire
- Machine Learning Model and AI
- Provide Executive Summary in JSON format
- C2 Communication Nodes Details

APIs

- Explore uses of other Databases and Messaging System for Vertical growth
- Include more measurement APIs for UI
- Allow notification using Email as well as SMS with Weekly reports.

UI

- Include Search functionality based on SHA256 of file as well as based on Threat type
- Allow information from outside world
- Show Executive Summary of Analysis Summary
- Display C2 communication Nodes graph

ArkThor

Segment

- **TEAM**
- **PROBLEM STATEMENT**
- **PUT YOUR BEST WORK ON DISPLAY**
- **PICTURE ABHI BAKI HAI MERE DOST**
- **THE BEST IS YET TO COME**
- **~~INTERROGATION~~ (Q&A)**

Open Forum

Don't wait any longer, head over to Github and/or DockerHub and get your hands on the **ArkThor product today!**

and be sure to provide feedback to help the product evolve and improve over time.

Arkthor.help@gmail.com

Thank you!

Okay, Okay

Sanitize and Validate

Good Morning Sir!

Sir, Can you explain again..

Is there going to be a quiz today as well?

Plain English

Hello World!

AIIMS

Whatever you say is correct!

Reverse Engineering

आज की सब्जी अच्छी नहीं बनी। Okay

Can you please mute your mic..

Thank you!

Arkthor.help@gmail.com