

Knight Foundation School of Computing and Information Sciences

Spring 2022 Capstone 2 Project

Ransomware Anomaly Detection

Students: Daniel Riquelme Rebollar

Mentor: Mike East, Kaseya; Carl Banzhof, RocketCyber

Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University

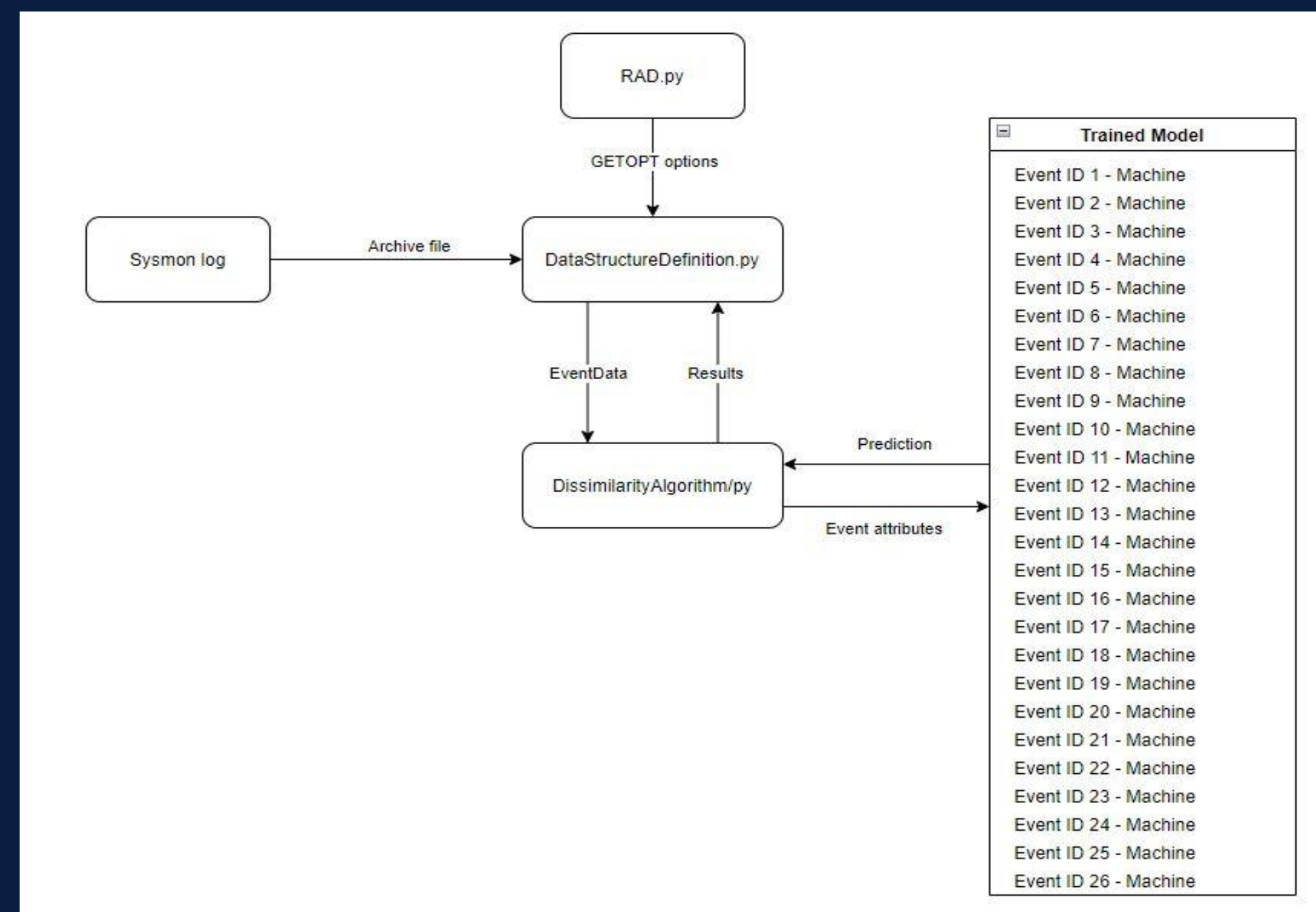
PROBLEM

According to the US chamber of commerce, a ransomware attack is a malicious access to an organization's network, systems and data with the purpose of encrypting or stealing data in exchange for a ransom. The malware enters the system through a phishing attack or a directed vulnerability exploitation.[1]

According to the latest statistics, ransomware attacks have become an increasingly important threat to commercial and government integrated systems in the last 10 years.

- In the first half of 2021, there were around 304.7 million ransomware attacks, which was a 151% increase from 2020.[2]
- In the same year, businesses and government departments had to pay on average \$1.8 million to recover their information. [3]
- In 2021, Kaseya, a software company, was attacked by the hacker group REvil. It infiltrated its IT infrastructure, and encrypted 1 million systems in exchange for \$70 million. It impacted more than 1000 client businesses.[2]

SYSTEM DESIGN



[IMV2] System's process flow

VERIFICATION

[illegible]

[IMV3] Model's accuracy with different thresholds.

ACKNOWLEDGEMENT

We thank Professor Masoud Sadijadi, and Mike East and for their assistance and mentorship that we received throughout the capstone 2 design project.

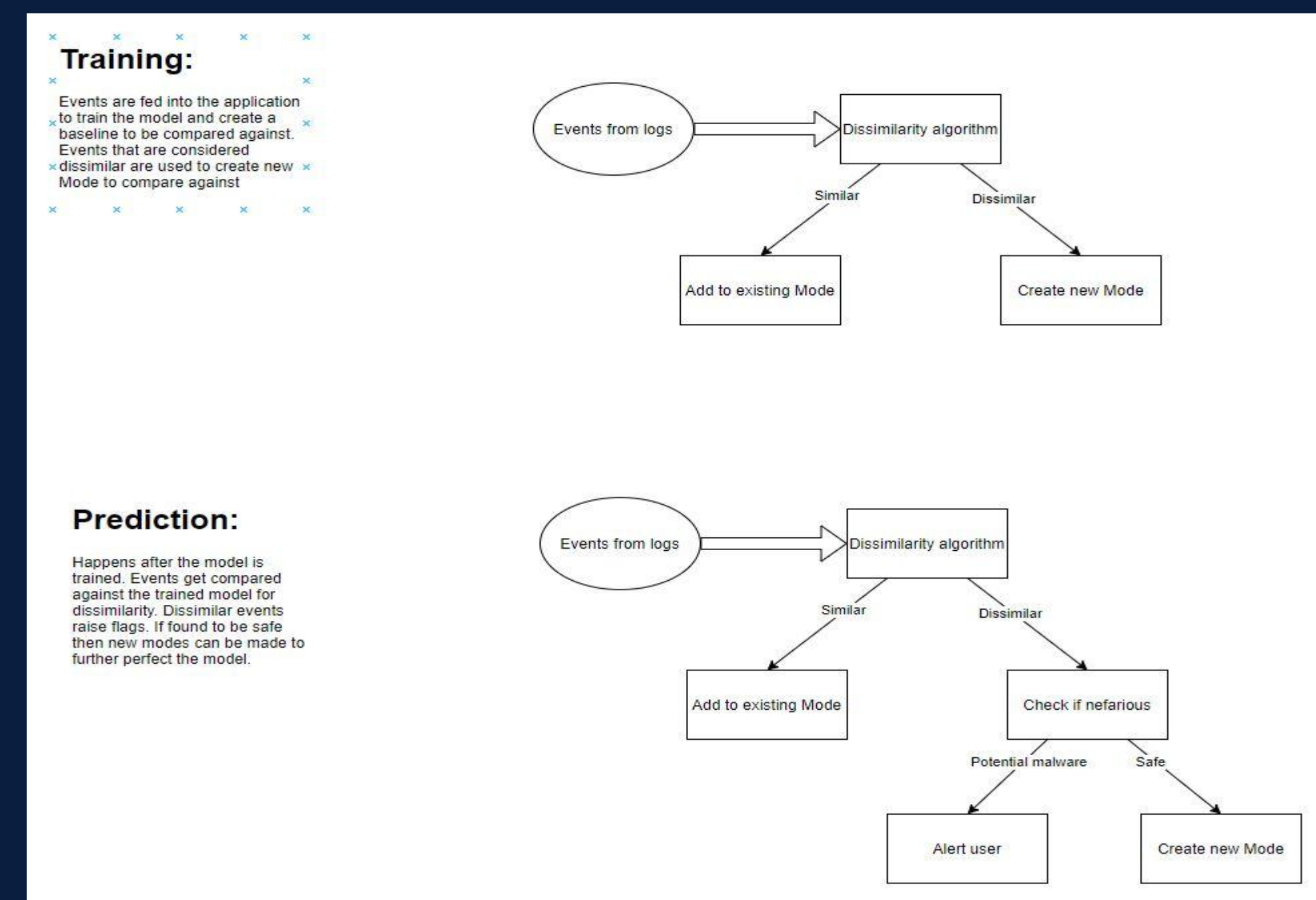
CURRENT SYSTEM

Modern ransomware attack systems involve use a combination of malware analysis and automation. There are three different techniques to detect malware in a system:

1. **Signature-based detection:** Called the first defense layer, it compares a ransomware sample hash to a system's known signature. Most antiviruses use this technique to make a quick systems scan.
2. **Behavior-based detection:** It involves the examination of new behaviors against historical entries. It relies on the examination of the file system, network traffic, and API calls.
3. **Deception-based detection:** It involves tricking the attacker in a controlled environment. One example is the use of Honeypots servers to avoid production attacks.

Our solution uses a behavior-based approach to create a machine learning model that can detect abnormal behavior. The Ransomware Anomaly Detection app trains a model using Windows Sysmon logs to train, and later predict possible attacks.

OBJECT DESIGN



[IMV3] System's modes.

SUMMARY

We were able to develop an initial functioning anomaly detection application using a trained dissimilarity algorithm. It can predict abnormal behavior using Sysmon Windows event logs. The user can easily interact with the application using CLI with different flags for a greater granularity.

Personally I was focused on the machine learning model, the Sysmon event ID's, and tools research team. I tested different unsupervised machine learning algorithms in order to choose the best fit. I tested K-means (5,10,50) clustering.

I also tested the different production code changes, and reviewed possible bugs solution.

REQUIREMENTS

The main project's requirement was to develop an initial integrated machine learning solution that was able to detect possible ransomware attacks in a network. It had to take into consideration the MITRE® ATT&CK framework [IM1] to develop a behavior based solution.

It included the research and local testing of machine learning algorithms, different approaches, and tools.

MITRE ATT&CK		Matrices Tactics Techniques Mitigation Groups Software Resources								
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Laterals Movement	Collection	Command and Control	Impact
Techniques	Techniques	Techniques	Techniques	Techniques	Techniques	Techniques	Techniques	Techniques	Techniques	Techniques
Density Compromise	Command and Scripting Interference	Account Manipulation	Abuse Elevation of Privilege	Abuse Elevation of Privilege	Brute Force	Account Discovery	Application Widenow	Active Collection	Command and Scripting Interference	
Exploit Public-Facing Application	Exploitation for Client Execution	BTFS Bypass	Account Token Manipulation	Account Token Manipulation	Credentials from Memory	Application Widenow	Internal Spearphishing	Audio Capture	Communication Channels	
External Remote Service	Inter Process Communication	External Authentication	Account Takeover	BTFS Bypass	Exploitation for Client Execution	Discovery	Reverse Binary Execution	Logon Session Collection	Data Exfiltration	
Hardware Additions	Native API	Boot or Logon Manipulation	Account Manipulation	Direct Volume Access	Forced Binary Execution	Cloud Service Dashboard	Reverse Binary Execution	Clipboard Data	Data Manipulation	
Phishing	Scheduled Task/Job	Service Disruption	Boot or Logon Manipulation	Service Disruption	Host Credential Access	Cloud Service Dashboard	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
Replication	Shared Modules	Browser Extensions	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
Removable Media	Software Deployment	Component Client	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
Service Disruption	System Services	Component Client	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
System Services	System Services	Component Client	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
Trusted Relationships	System Services	Component Client	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
Valid Accounts	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	
	Windows	External Services	Service Disruption	Service Disruption	Man-in-the-Middle	File and Directory Discovery	Reverse Binary Execution	File and Directory Discovery	Data Manipulation	

[IMV1] MITRE® ATT&CK Matrix framework

IMPLEMENTATION

Model:

- Dissimilarity Algorithm-String Comparison.

Hardware:

- Requires a machine with at least Windows 10 OS.

Software:

- Windows Sysmon logging tool.
- Python 3.10.
- Visual Studio Code.
- GitHub versioning system.

REFERENCES

- [1] Staff, U. S. C. (2022, April 13). Understanding ransomware attacks. U.S. Chamber of Commerce. Retrieved April 10, 2022, from <https://www.uschamber.com/security/cybersecurity/ransomware-joint-blog-pci-ssc-and-u-s-chamber-of-commerce>
- [2] Edwardson, C. (2021, July 28). Record 304.7 million ransomware attacks Eclipse 2020 global total in just 6 months. SonicWall. Retrieved February 10, 2022, from <https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks-eclipse-2020-global-total-in-just-6-months/>
- [3] Person. (2021, December 6). Ransomware attacks soar, hackers set to become more aggressive - canada spy agency. Reuters. Retrieved February 10, 2022, from <https://www.reuters.com/technology/ransomware-attacks-soar-hackers-set-to-become-more-aggressive-canada-spy-agency-2021-12-06/>