FINAL REPORT

Technology stack : AI for cyber security with IBM Qradar project title : Advanced techniques in Rule creation for threat, Detection

Team ID : LTVIP2024TMIDI2665

Team NO : 1

Team Members : 1

1. Manpu KANVITH

COLLEGE : DR LANKAPALLI Bullayya COLLEGE

VISHAKHAPATNAM

Index

Introduction:

Cyber threat actors conduct Malicious cyber threat activity by exploiting technical vulnerabilities employing social Engineering techniques, or by Manipulating Social Medial. A determind and capable adversary will often carefully select the technique most likely to result in succesfull Exploitation after conducting reconnaissance against their target and may use a range of techniques to achive their goal.

Abstract:

Cyber incidents that targets ICSs are security, S safety and business problems. Such abnormal events affect physical devices, such as actuators and sensors. if a cyberattack results in manufacturing operations being shut down. a company will lose significant revenue. On addition, if a cyber attacks targets systems that require safety operations, the operations will be endangered. so far, cyberattacks on an iron furnace have been reported On addition to safety risks cyber attacks continues to pose serious financial risk for companies (3) therefore cyber attacks should be prevented to ensure corporate resilience

Stage 1:

Title of the project : Advanced technique in Rule Creation for threats

Cyber threat actors are not equal in terms of capability and sophistication, and have a range of resources, training, and support for their activity. Cyber threat actors may operate on their own or as part of the larger organization. Sometimes, even sophisticated actors are less because they can still be effective for a given task and/or make it difficult for defenders to attribute the activity. Nation-states are frequently the most sophisticated threat actors, with dedicated resources and personnel and extensive planning and coordination.

Stage 2:

Types of threats:

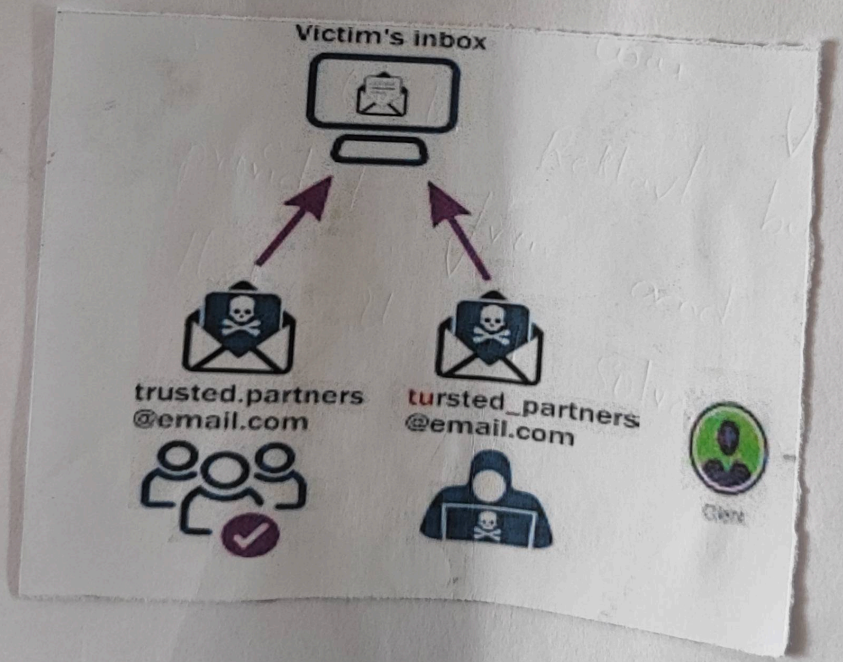
In the simplest sense, a cyber security threat, or cyberthreat, is an indication that a hacker or malicious actor is an indication that a hacker or to a network for the purpose of launching a cyber attack.

Malware:

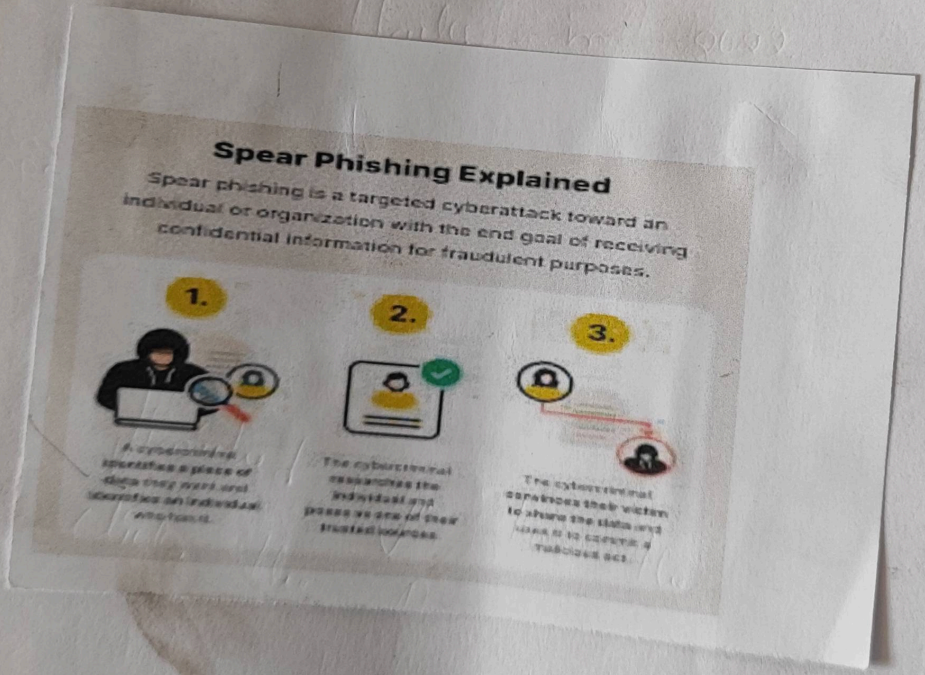
Common types of Malware include;

Ransomware; locks a victim's data or device and threatens to keep it locked, or leak it publicly unless the victim pays a ransom to the attacker. According to the 2BN Security X-Force threat Intelligence Index 2023, ransomware attacks accounted 14 percent of all cyber attacks in 2022.

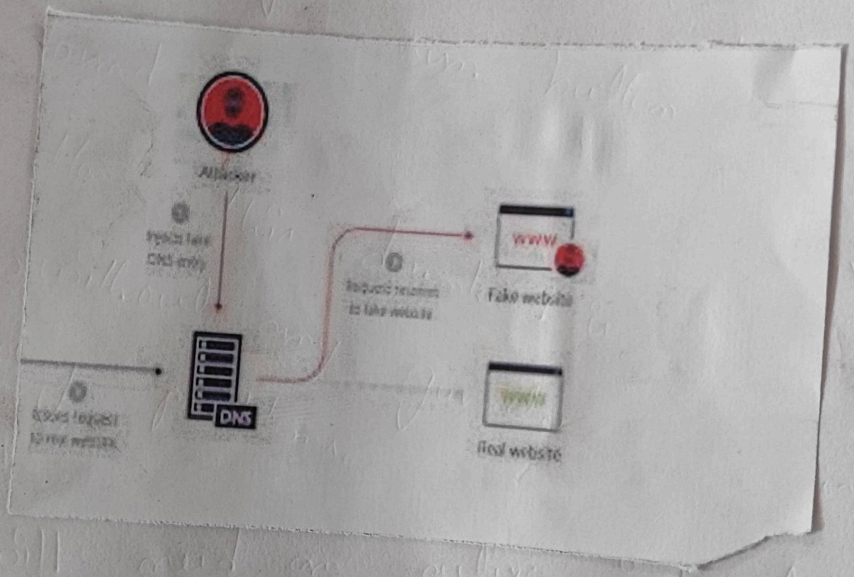
Common types of phishing include;



What is phishing & Spear phishing that targets corporate executives or wealthy individuals Business Email Compromise - Scam in which Cybercriminals vendors or trusted business associates to trick victims into writing money or sharing sensitive data.



programs, this a good choice. It's free, and it does exactly what it promise. But it was not designed to be a on stop solutions.



Page 3: Tools in of the threat in cyber security)

Tools used in Cyber Security

GMER is a anti-rootkit Scanner that Searches your computer for Rootkit that infect the Master Boot Record, or MBR, of your computer. This includes the TDL4/3, MBRoot and whitter rootkits for this program to properly work it must first download the Avast virus definitions, so you will need an active internet Connection before using it. A rookit is a Malware program that is designed, so you typically harder to remove them generic Malware, which is the reason that stand-alone utilities such as TDSS killer have been.

→ When the scan is finished, go to the Script lab and click the Run button if anything was found.

→ Click Restart button. This download is provided free and without any guarantee that it will solve any problems.