Training course outline

ITU and Naif Arab University for Security Sciences (NAUSS)

Title	**Ransomware Analysis: File encryption and decryption mechanism.**
Modality	Online Instructor led
Dates	6-7 June 2022
Duration	2 days
Registration deadline	30 May 2022
Training fees	0 USD (Free)
Description	Ransomware is major techniques that is used by cyber attackers. Victims of Ransomware usually paid their money to attackers for decrypt their valuable files encrypted by Ransomware. This training will enable the participants to understand knowledge of types of Ransomware, encryption, and decryption mechanism of Ransomware. This course also provides hands-on practice with a virtual machine for encryption and decryption techniques used by Ransomware
Code	22OI28036ARB-E

1. LEARNING OBJECTIVES

To understand ransomware types and trends and their encryption and decryption mechanism with hands on exercise.

2. LEARNING OUTCOMES

By the end of this training, participants should be able to have:

- Knowledge of Ransomware definition and objective.
- Knowledge of types and trends of Ransomware.
- Knowledge of encryption and decryption mechanism used by Ransomware.
- Knowledge of Windows file format.
- Skills to conduct of encryption and decryption.
- Skills in compare between Ransom file and common file with hex view tool.
- Skills in using virtual machine.

3. TARGET POPULATION

This training is providing a great value for security managers, engineers, technical staff, telecom operators, administrators from government organizations, industry companies and academia, as well as individuals who are interested in Ransomware cyber-attacks.

4. ENTRY REQUIREMENTS

There is not mandatory prerequisite course to attend this course, but the following knowledge and skills preferred:

- Have a background of computer science and IT related experience.
- Basic knowledge about windows operating system

5. TUTORS/INSTRUCTORS

Name of tutor(s)/instructor(s)	Contact details
Dr. Kyounggon Kim	kkim@nauss.edu.sa

6. TRAINING COURSE CONTENTS

Topic	Description
Ransomware definition	Explain a definition and an objective of Ransomware
Ransomware history, types, and trends	Explain the Ransomware types and evolution of their techniques.
Ransomware operating process	Explain the Ransomware process such as finding valuable file, encryption, and require digital money
Encryption and decryption	Explain the encryption and decryption mechanism of Ransomware with hands-on encryption and decryption such as AES and RSA used in Ransomware.

7. TRAINING COURSE SCHEDULE (Riyadh Time)

Day / Session	Time	Topic	Exercises and interactions
Day 1: 06 June 2022	9:00 to 13:00	Ransomware introduction Windows Registry	Ransomware definition, types, and trends analysis.
Day 2: 07 June 2022	9:00 to 13:00	Encryption and Decryption	Analysis of Ransomware operating process. Exercise AES cipher and RSA cipher algorithms.

8. METHODOLOGY (Didactic approach)

This course provides Instructor-led presentations and provides hands-on practices. Some hands-on practices will provide pre-recorded files.

9. EVALUATION AND GRADING

Evaluation for this course is conducted by final overall exam (100%): Participants should attend final exam at the end of this course. A passing mark of 70% is required to get the course completion.

10. TRAINING COURSE COORDINATION

Training Coordinator:	**ITU Coordinator:**
Dr. Abdulrazaq Al-Morjan Director of Centre of Excellence in Cyber Crimes and Digital Forensics, at NAUSS Mobile: +966 54 470 05 53 Email: t-aalmargan@nauss.edu.sa	**Mr. Ahmed El Raghy** Senior Advisor ITU Arab Regional Office Tel: +202 3537 1777 Mobile: +201005281908 Fax: +202 3537 1888 Email: ahmed.elraghy@itu.int