

ICT: Emerging Technological Trends and Society

TuK



Btech IT/CT/CCN Year IV term 3

003: COMPUTER **MANAGEMENT TRENDS**

SUBJECT CODE: ECII/ECSI/ECCI 4204

COMPUTER

MANAGEMENT

TRENDS

LECTURE OVERVIEW

- 1. Lecture Aims & Objectives**
- 2. Lecture Outline**
- 3. Recommended chapter from recommended reading list**
- 4. Lecture Topic**
- 5. Q&A**

COMPUTER MANAGEMENT TRENDS

- AIMS & OBJECTIVES

- 1) To study past and present **TRENDS** in traditional, current and future **computer management**
- 2) To learn future trajectories of growth projected **for** emerging **trend in computer management**
- 3) To identify and explain the characteristics, **advantages and disadvantages** of computing management **trends**
- 4) To discuss the social and ethical implications on society related to **trends in computer management**

COMPUTER MANAGEMENT TRENDS

- 1) introduction to topic and why study computer management trends?
- 2) What is computer management?
- 3) Current best practises in computer management?
- 4) Future emerging trends in computer management
- 5) Q & A

COMPUTER MANAGEMENT TRENDS

>>>Endpoint management s/w (EMS):-s/w for device governance and compliance i.e.

(i) Track devices in M.U.C.E.

(ii) Ensure h/w, s/w & n/work is secure and up-to-date

COMPUTER MANAGEMENT TRENDS

>>>EMS purpose:-

- ❑ Manage endpoint assets connected to a network**
- ❑ Manage patch updates**
- ❑ Ensure device compliance**
- ❑ Detect new/suspicious devices connected to a network**
- ❑ Install new OS or applications to an endpoint device**



Wana Decrypt0r 2.0



Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

DEFINITION:-RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

- Use of malicious software
- Break into, encrypt and hold data ransom
- Home router the target of attack (why? how?)
- Role of cryptocurrency:- making RAAS easier for cybercriminals (how? why?)

DEFINITION:-RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

- World emerging from COVID-19 coronavirus pandemic lockdowns
- New Pandemic:-COVID-19 ransomware attacks**
- May lead to a new internet(meaning?)**
- Data breaches and security incidents now commonplace
- Every week a new cyber attack

DEFINITION:-RANSOMWARE-AS-A-SERVICE (RAAS) MODEL

- 2016: Cyber attack every 40 seconds
- 2019: Cyber attack every 19 seconds
- 2021: Cyber attack incident every 11 seconds.
- 2021: \$350 million in ransom payments to ransomware gangs
- 2022: Attacks costs \$6.1 trillion (Ksh 717,431,980,00.00/=)
- Cybercrime = third-largest economy after U.S & China.

SOPHISTICATED MALWARE AND ROUTERS:-RANSOMWARE-AS-A-SERVICE (RAAS)

- Custom-built remote access malware
- Written for MIPS architecture
- Compiled for small office and home office routers
- Infects routers by Cisco, Netgear, Asus, DrayTek etc.
- Controls connected devices running Windows, macOS, Linux

SOPHISTICATED MALWARE AND ROUTERS: RANSOMWARE-AS-A-SERVICE (RAAS)**MODEL**

- 1) Enumerate devices connected to infected router
- 2) Collect DNS lookups and all network traffic
- 3) Undetectability
- 4) installation of other malware
- 5) DNS hijacking and HTTP hijacking
- 6) Cripple Internet services:

RANSOMWARE-AS-A-SERVICE (RAAS) DEFENCE MODEL:

- 1) Multi-factor authentication:
- 2) Avoid Shadow I.T.- (What is it? how? why?)
- 3) Reboot:-
- 4) Factory reset.

QUESTION AND ANSWER SESSION

ANY
QUESTIONS
?