

# CSF Group Assignment

By:

IT03

Branson Ng Jun Hao (S10219122G)

Tan Jin Daat (S10222867E)

Koh En Yang (S10222282K)

Sim Yuan Yee(S10223521F)

# Table Of Contents

## **Unit 1**

About the Attack And Damages

## **Unit 2**

How The Attack Took Place

## **Unit 3**

Security Domains Involved

## **Unit 4**

Action Taken By Authorities  
and Status

## **Unit 5**

Related Attack

## **Website**

Explanation of pages and  
Functions

# UNIT 1:

## About the Attack and The Damages



Introduction

01

Exploit Explanation

02

Impact Of The Attack

03

# UNIT 1

## About the Attack and The Damages

### ***Introduction***

The Wannacry attack was a ransomware attack in 2017 which encrypted files in order to extort victims for money

### ***Exploit Explanation***

The WannaCry Attack utilised crypto ransomware, which is a type of malware that is used to extort victims for money by encrypting their files on the affected computers.

### ***Impact Of The Attack***

The damage done by WannaCry was immense and multinational, with Europol stating that the attack was on an "unprecedented level"

# UNIT 2:

## How the Attack took place



When The Attack  
Took Place

01

Who Were At The  
Highest Risk

02

Which Vulnerabilities  
Were Exploited

03

# UNIT 2

## How the Attack took place

### ***When The Attack Took Place***

The WannaCry Attack took place on 12th of May 2017 with the initial attack taking place in Asia.

### ***Who Were At The Highest Risk***

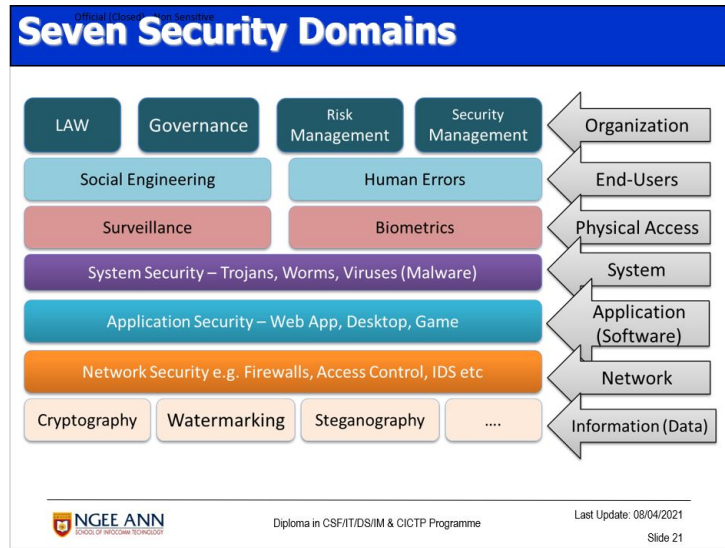
Users using Windows XP and Windows Server 2003 were at particularly high risk

### ***Which Vulnerabilities Were Exploited***

The vulnerability WannaCry exploits lies in the Windows implementation of the Server Message Block (SMB) protocol.

# UNIT 3:

## Security Domains Involved



The 7 Security Domains In Cybersecurity

01

Security Domains Involved In The Attack

02

Loss From The Attack

03

# UNIT 3:

## Security Domains Involved

### *What Security Domains Are*

There are 7 Security Domains in Cybersecurity  
Organization, End-user,  
Physical Access, Software,  
System, Network, Data

### *What Security Domains Were Affected*

3 Security Domains were compromised in the  
WannaCry Attack  
End-Users , Organization,  
Systems

### *Loss From The Attack*

Large Amount of money and resources was lost due to the attack  
(\$4Billion)

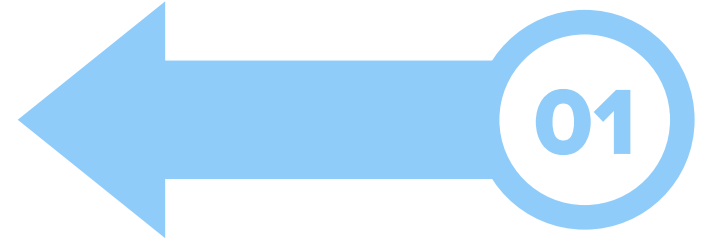


# UNIT 4:

## Action taken by the authorities and status



When The Attack  
First Began



How The Attack  
Was Defeated



Hackers  
Attempts



# UNIT 4

## Action taken by the authorities and status

### *When the attack first began*

Microsoft issued an security update for their Windows XP, Windows Server 2003 and Windows 8 to combat the malware

### *How the attack was defeated*

A researcher named Marcus Hutchins found a killswitch located the domain

### *Hackers attempts*

Attackers tried using a mirai botnet variant to overwhelm the domain but Hutchins switched to a cached version which can handle higher traffic

# Unit 5:

## Related Attack



**A Similar Attack**

**01**

**How did it happen**

**02**

**What Is The Current Status On The Other Attack**

**03**

# UNIT 5

## Related Attack

### *A Similar Attack*

Another example of a ransomware crypto worm is ZCryptor.

### *How did it happen*

For the first attack, it acted as a popular program and infected the system through malicious macros in a Microsoft Office file

### *What Is The Current Status On The Other Attack*

Experts have not been able to find way to decrypt the files and let the affected users bypass the ransom option.

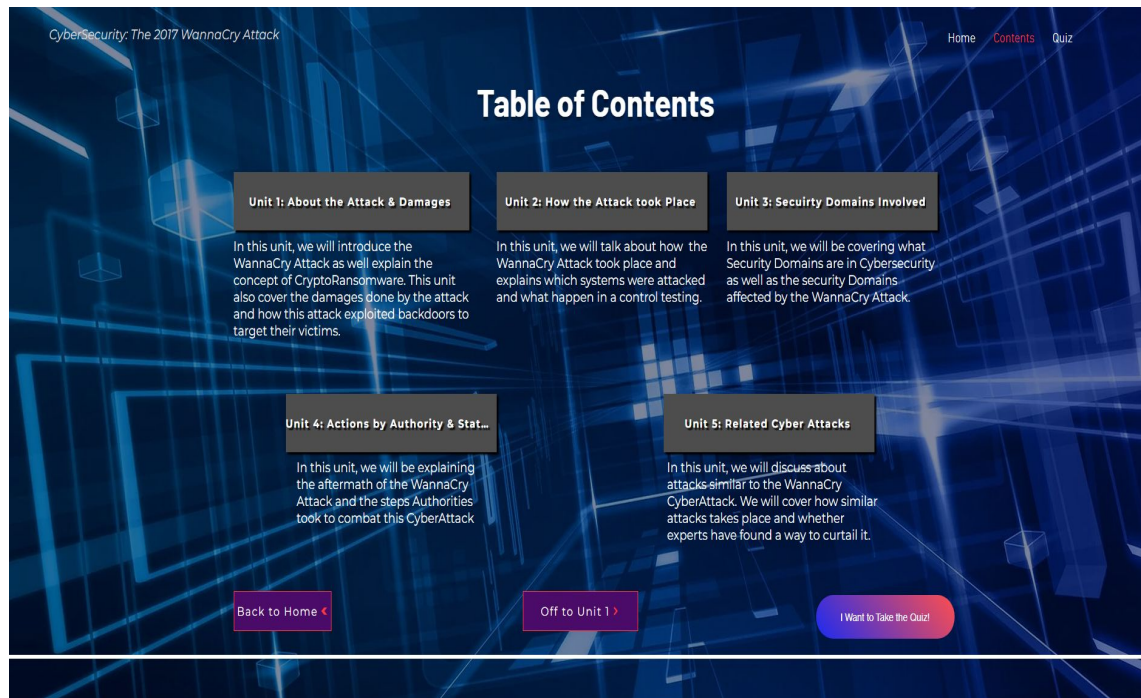
# Home Page

- Title Header
- Short description of what users will be learning



# Table Of Contents Page

- Links for each unit
- Short description for each unit
- Quiz Link
- Unit by Unit link



# Unit Page

- Executive Summary is provided
- 3 Key Learning Points are highlighted in text
- 1-2 Teaching Videos are provided: a live sketching video and a slide deck presentation for learners with different preferences

The screenshot shows a webpage titled 'CyberSecurity: The 2017 WannaCry Attack'. The main heading is 'Unit 1: About the Attack and Damages'. Below this, a welcome message states: 'Welcome Cyber Explorer! In this unit we will be introducing to you what the 2017 WannaCry Attack is and the concept of Crypto Ransomware. Click the videos on the right to find out more!'. To the right of the text are two video thumbnails: the top one shows a hand sketching on a whiteboard, and the bottom one is a black slide deck. Below the videos, a section titled 'Key Learning Points from this Unit:' lists three points: 1. WannaCry was an extremely dangerous attack which targeted high-level institutions including Government assets. 2. Crypto Ransomware uses encryption to extort victims for money in exchange for the decryption of files. 3. Backdoors are exploited which allowed the attackers to access victim's computer without authorization. At the bottom of the page are two purple buttons: 'BACK TO CONTENTS' and 'GO TO NEXT UNIT'. A navigation bar at the top right contains links for 'Home', 'Contents', and 'Quiz'.

CyberSecurity: The 2017 WannaCry Attack

Home Contents Quiz

## Unit 1: About the Attack and Damages

Welcome Cyber Explorer! In this unit we will be introducing to you what the 2017 WannaCry Attack is and the concept of Crypto Ransomware. Click the videos on the right to find out more!

Key Learning Points from this Unit:

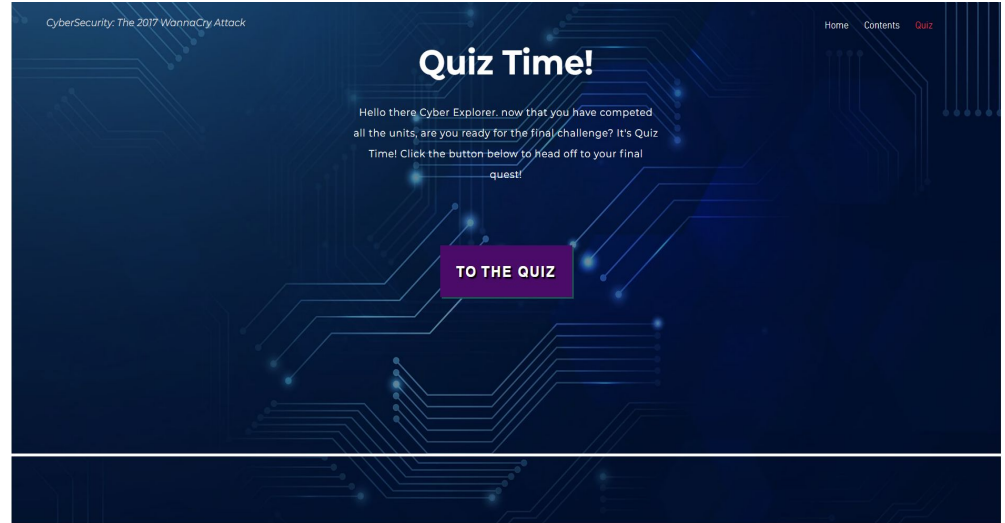
1. WannaCry was an extremely dangerous attack which targeted high-level institutions including Government assets.
2. Crypto Ransomware uses encryption to extort victims for money in exchange for the decryption of files.
3. Backdoors are exploited which allowed the attackers to access victim's computer without authorization.

BACK TO CONTENTS GO TO NEXT UNIT



# Quiz Page

- Total of 5 questions
- MCQ with 3 choices each
- Total score out of 5 would be displayed at the end



1) What caused The 2017 WannaCry Attack?

☐ Cause by Crypto Ransomware

☐ Caused by Social Engineering

☐ Caused by physical breach in security



# Sources

[https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

[Ransomware WannaCry: All you need to know | Kaspersky](#)

[The NHS cyber attack: how and why it happened, and who did it \(acronis.com\)](#)

<https://digi117.com/wp-content/uploads/2018/08/2018.08.08-Software-Security-How-To-Secure-Your-Code-And-Improve-The-Security-Of-Your-Software-900x600.jpg>

# HyperLinks

<https://s10222867.wixsite.com/the2017wannacry>

# Thank You!

Does anyone have any questions?