Threats to Data

Unit R012 - Understanding tools, techniques, methods and processes for technological solutions

Introduction

- With any computer system there are a number of threats to data that could occur. These are:
  1. Botnet
  2. Malware
  3. Social engineering
  4. Hacking
  5. Distributed Denial of Service (DDoS)
  6. Pharming

Botnet

- A botnet is usually the result of several computers being infected by a bot malware.
- You will look at these shortly.
- Being infected with a botnet will allow the person who created it, to take control of the computer system.

Malware

- Malware is malicious software that is installed on a computer system that collects information about users without their knowledge.

- There are many types of malware:
  a) Adware
  b) Bot
  c) Bug
  d) Ransomware
  e) Rootkit
  f) Spyware
  g) Trojan Horse
  h) Virus
  i) Worm
-

Malware

Type of Malware	Why it is used?	How it works?	How to mitigate?
Adware	Adware makes money for the creator	Adware is also known as advertising supporting software. This is any software that automatically shows adverts and pop ups etc. Most adware is harmless but some may include spyware like key loggers etc.	Install, run and keep updated a security software package Do not open files from unknown sources Do not click any links in emails.
Bot	Bots take control of a computer system	A bot allows an attacker to take control of the affected computer without the users knowledge. It can result in a botnet which is a interconnected network of infected machines.	Install, run and keep updated a security software package Do not open files from unknown sources Do not click any links in emails.
Bug	Bugs are connected to software and are a flaw that produces an unwanted outcome.	Bugs are usually the result of human error when coding the software. They can usually be fixed by the creator issuing a fix or a patch. They can allow attackers to bypass security, override privileges or steal data.	Check for and install any patches that are released from software creators.

Malware

Type of Malware	Why it is used?	How it works?	How to mitigate?
Ransomware	Ransomware holds a computer system captive and demands a ransom to release it.	Ransomware can restrict user access to the computer system by encrypting files or locking the system down. A message is usually displayed to force the user to pay the ransom to get the restrictions lifted.	Do not open any files from an unknown source. Do not click links in emails. Install, run and keep updated a security software package.
Rootkit	A rootkit is design to remotely access or control a computer without being detected by the security software.	When installed a rootkit can enable an attacker to remotely access files, steal data, modify configurations or control the computer.	Keeping security software up to date. Not downloading suspicious files.
Spyware	Spyware can collect data from an infected computer including personal information like log in details and financial records.	Spyware is usually hidden from the user and can be difficult to detect. Some spyware like key loggers may be monitoring the users. Spyware can install additional software or redirect the user to different websites.	Do not open any files from an unknown source. Do not click links in emails. Install, run and keep updated a security software package.

Malware

Type of Malware	Why it is used?	How it works?	How to mitigate?
Trojan Horse	A trojan-horse is a standalone malicious software that is designed to give full control of a machine to another.	Trojans often appear to be something that is wanted by the machine. They can be hidden in valid programs and make copies of themselves, steal information or harm the host machine.	Do not open any files from an unknown source. Do not click links in emails. Install, run and keep updated a security software package.
Virus	A virus makes an attempt to make a computer system unreliable.	A virus is a computer program that replicated itself and reads from machine to machine. Viruses can infect other machines by infecting files that are accessed by other machines	Do not open any files from an unknown source. Do not click links in emails. Install, run and keep updated a security software package.
Worm	A worm is a standalone computer program that replicates itself so it can spread to other computers	A worm can use a computer network to spread. Unlike a computer virus, it does not need to attach itself to an existing program. Worms will cause harm to a computer system even if only by consuming bandwidth	Do not open any files from an unknown source. Do not click links in emails. Install, run and keep updated a security software package.

Social Engineering

- Social Engineering is the art of manipulating people so that confidential information can be found out.

- It can take many forms such as:
  - Phishing
  - Pretexting
  - Baiting
  - Quid Pro Quo
  - Tailgating/Piggybacking
  - Shoulder surfing

Social Engineering

Type of Social Engineering	Why it is used?	How it works?
Phishing	Phishing tries to get users to input their credit or debit card numbers, or security details or log in details into a fake website.	Phishing uses a fake website that looks identical to the real one. Common targets for phishing are banks and insurance websites. Attackers send out emails or texts from pretending to be banks, with fake links that takes the user to a fake website.
Pretexting	Pretexting is when a cyber criminal lies to get data or information.	This is a scam where the criminal pretends to need the information to confirm the identity of the person that they are talking to.
Baiting	Baiting tries to get victims to give cybercriminals the information they need.	Baiting is similar to phishing. Cybercriminals promise of goods to get the information that they need. E.g. Free downloads in exchange for log in details.

Social Engineering

Type of Social Engineering	Why it is used?	How it works?
Quid Pro Quo	Quid pro quo tries to disable anti virus software updates so that malware can be installed to gain access to the system.	Similar to baiting except the promise is for a service rather than goods. A method is a phone call pretending to be an IT service provider offering assistance to fix problems.
Tailgating/ Piggybacking	Tailgating or Piggybacking means trying to gain access to a secure building or room.	The most common type of this is an attacker pretending to be a delivery driver and asking an authorised person to hold the door.
Shoulder surfing	Shoulder surfing aims to steal data and information	This is where private and confidential information is seen. E.g. An attacker may stand very close to someone using a cash machine in order to see their pin.

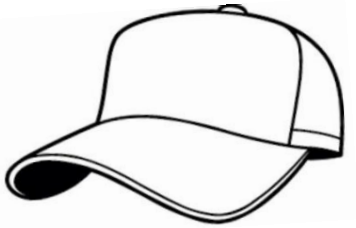
Hacking

- Hacking means finding weaknesses in an established system and exploiting them to gain unauthorised access.

- A hacker may be motivated by money, protest or challenge.

- There are three types of hacking:
  - White Hat Hacking
  - Grey Hat Hacking
  - Black Hat Hacking

Hacking



- **White Hat Hacking**
  - This is where the hacker is given permission to hack into systems to identify any loopholes or vulnerabilities.
  - As this type of hacking is done with permission, it does not break any laws
- **Grey Hat Hacking**
  - This is where the hacker hacks into computer systems for fun or to troll but without malicious intent.
  - If a grey hat hacker finds a weakness they may offer to fix it for a fee.
- **Black Hat Hacking**
  - This is where the hacker hacks into a computer system with malicious intent.
  - This intent can include theft, exploiting the data stolen and selling the data on.
  - Black hat hackers carry out illegal hacking and can be prosecuted under UK law.

Distributed Denial of Service (DDoS)

- Distributed denial of service is an attempt to make a computer or network system unavailable to its users by flooding it with network traffic.
- A DDoS is usually focused on preventing an internet site from functioning efficiently, or at all, either temporarily or forever.
- Attackers usually target sites hosted by high-profile web servers such as banks, payment websites and mobile phone companies.

Pharming

- Pharming is a cyber-security attack that tries to redirect visitors from a genuine website to a fake one.
- This is done without the knowledge or consent of the users.
- There are some similarities between phishing and pharming.
- Fraudulent websites are used by attackers carrying out both phishing and pharming attacks, but phishing attacks use fake or hoax emails.