DFA – Module 1 : part 5
Cyber Crime, Incidence Response system (07.02.22)

Arijit Chakraborty

Feb 7, 2022

Data = Oil , Apps = Engine

- Revolution in Fintech, edutech industry: inclusive approach
- Agro-tech : Data wave on weather, cropping, sowing, watering, harvesting (precision agriculture : AI app)
- Pharma & healthcare – increasing digitisation
- Central & State Government services – data driven, Bchain tech
- Digitisation for MSME

Understanding Cyber Crime

- ***Cyber Dependent Crimes =***
- digital system is the target as well as the means of attack.
- attacks on computer systems to disrupt IT infrastructure,
- stealing data over a network using malware (purpose of the data theft is usually to commit further crime).
- ***Cyber Enabled Crimes***
- 'Existing' crimes that have been transformed in scale or form by their use of Internet.
- Use of Internet to facilitate drug dealing, people & Arms / weapons trade/ smuggling etc

Cyber Crime – Motivation

- Money/Greed
- Curiosity
- Revenge
- Fun
- Praise seekers
- Passtime
- *Girls = most found victims of cyber crimes*

CYBER CRIMES

E-Mail bombing:

sending a large amount of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

Data diddling:

altering raw data just before it is processed by computer and then changing it back after the processing is completed.

Salami attacks:

to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer

Denial of Service:

flooding computer resources with more requests than it can handle, causes resources to crash thereby denying authorized users the service offered by the resources.

MALWARE

- **Examples**
- Ransomware
- Adware
- Botnets
- Rootkits
- Spyware
- Viruses
- Worms

RANSOMWARE

- **Examples**

- Cryptolocker
- Winlock
- Cryptowall
- Reveton
- Bad rabbit
- Crysis
- Wannacry

Why Hacking ?

- Money extortion
- For Fun
- To Show-off
- Stealing confidential information
- To hamper privacy
- To damage System functioning
- To test security of the system

Attack Descriptions

- **Denial-of-service (DoS) –**
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS) –**
- a coordinated stream of requests is launched against a target from many locations at the same time

Leading Threats: Viruses

- **Vital Information Resource Under Siege (VIRUS)**
- A virus attaches itself to a program, file, or disk.
- When the program is executed, the virus activates and replicates itself.
- The virus may be benign or malignant but executes its payload at some point (often upon contact).
  - Viruses can cause computer crashes & loss of data.
- **Defence : Recover or prevent virus attacks:**
  - Avoid potentially unreliable websites/emails.
  - Re-install operating system.
  - Use and maintain anti-virus software.

Why attack with Viruses?

- ✓ To distribute political message.
- ✓ To attack products, service delivery & reputation of specific companies.
- ✓ Some hackers consider their creations to be works of art,
- ✓ Some hackers see ‘virus attack ‘ as a creative hobby.
- ✓ Financial gain from identity theft

Logic Bombs and Trojan Horses

Logic Bomb: Malware logic executes upon certain conditions.

Examples:

Software which malfunctions if maintenance fee is not paid.

Employee **triggers a database erase** when he is fired.

Trojan Horse: Masquerades as a benign program while quietly destroying data or damaging system.

Download a game: It may be fun but contains hidden code that gathers personal information without your knowledge.

Threat of **Online gaming Websites / apps**

Social Engineering

- Social engineering manipulates people : performing actions or divulging confidential information.
- Similar to a confidence trick or simple fraud,
- Use of deception to gain information, commit fraud, or access computer systems.

Pharming: Counterfeit Web Pages

Phishing: Counterfeit Email

- **MITM**
- An attacker pretends to be your final destination on the network.
- When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.

Impersonation

- Impersonators ; Issue for popular personalities, influencers, activists & corporates/businesses as they mimic a legitimate account for various reasons.
- **Reasons :**

✓ pure-play parody accounts,

✓ doing mischief or a crime,

✓ financial fraud.

- Some accounts created by **fans of popular personalities**,
- Some **run through bots**
- Some fake account holders **add own image to Celebrity s picture** by morphing original content in order to **claim proximity, & get favours**.

Ransomware

- This sort of attack **encrypts data and renders it unusable until the victim pay the a ransom**.
- The best way to avoid an attack with ransomware is **to have real-time security protection, and hiring an IT security specialist** to perform regular backup routines.
- The best option is to act before cyber security is at risk and protect most important data before it becomes an issue.

Cyber Extortion - *Ransomware*

- Normally loaded onto a computer via a download/attachment/link from an email or website.
- Will either lock the screen or encrypt data.
- Once Ransomware is uploaded on computer/tablet/phone it is very difficult to remove without removing all of the data
- Wannacry attack 2017 - One of the biggest cyber attacks
- hit 300,000 computers in 150 countries.
- Companies affected: Renault, FedEx, Spanish telecoms and gas companies, German railways.
- **Spyware / Adware**
- To take control of computer and/or to collect personal information without user's knowledge. Ex- Pegasus
- **Impersonation on Social media**