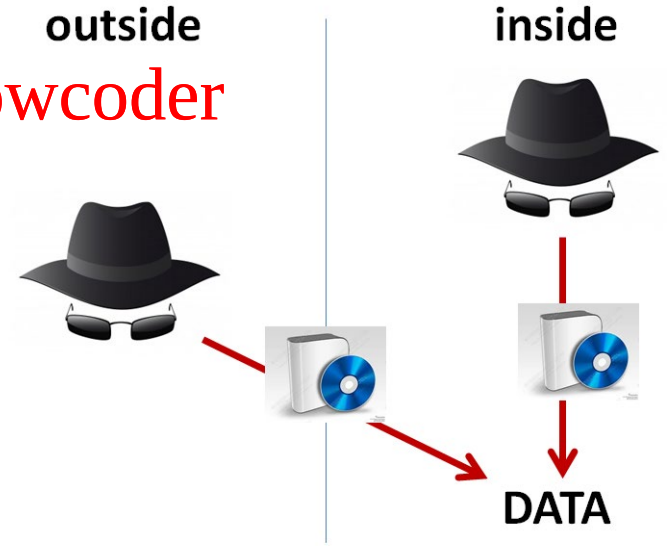
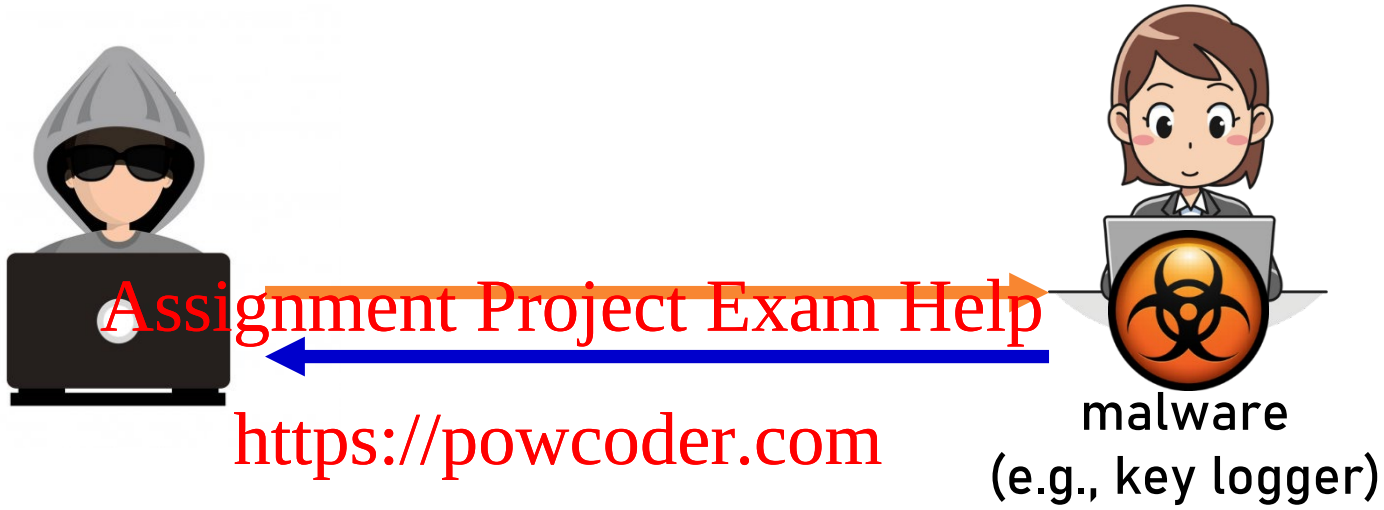
Threat Events: Software Attacks

- **Deliberate Software Attacks**
  - a deliberate action aimed to violate / compromise a system's security through the use of specialized software
  - types of attacks base on the type of malicious software:
    a) Use of Malware
    b) Password Cracking
    c) DoS and DDoS
    d) Spoofing
    e) Sniffing
    f) Man-in-the-Middle
    g) Phishing
    h) Pharming

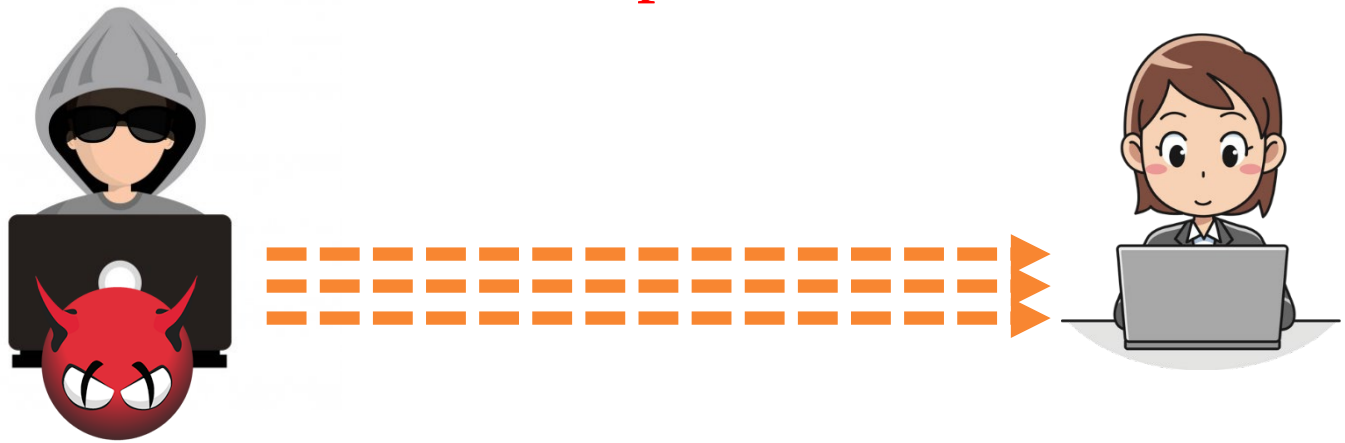


Threat Events: Software Attacks



https://powcoder.com

Add WeChat powcoder



malicious software
(e.g., DDoS program)

Threat Events: Software Attacks (cont.)

Hacker = person that conducts a deliberate software attack

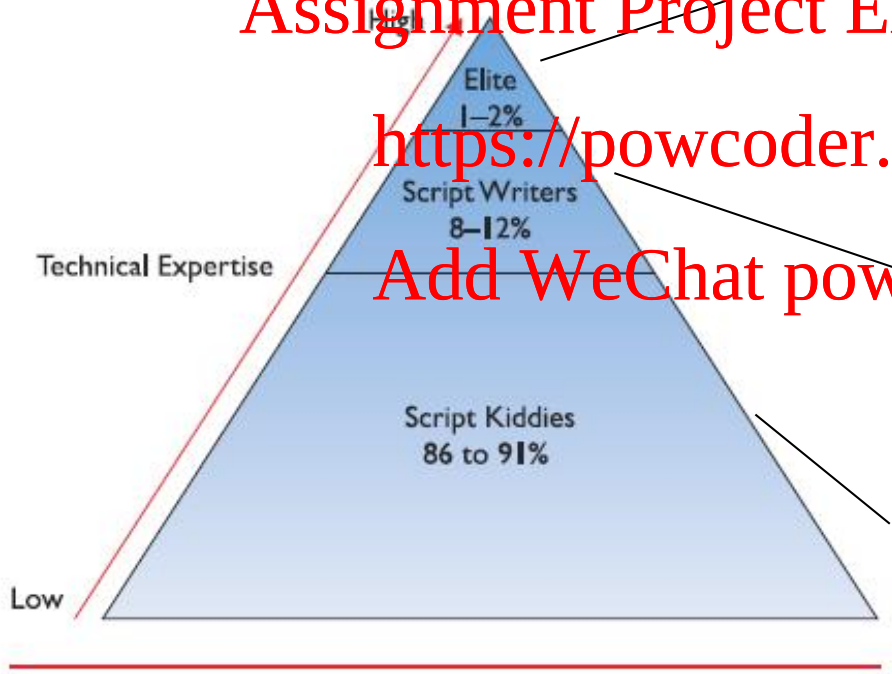


Figure 1.1 Distribution of attacker skill levels

Elite Hackers: Individuals capable of **discovering new vulnerabilities** and writing programs (scripts) that exploit those vulnerabilities.

Script Writers: Individuals capable of writing scripts to exploit known vulnerabilities.

Script Kiddies: Individuals with (only) enough understanding of computer systems to be able to download and run scripts that others have developed. Vast majority of attack activity on the Internet is carried out by these individuals.

Threat Events: Software Attacks (cont.)

'good guys' hired to discover security vulnerabilities in a system

illegally access a system, but generally do not exploit the discovered vulnerability

'bad guys' (criminals) use their skills to conduct malicious activities

Threat Events: Software Attacks (cont.)

Example: Grey Hat Hackers …

October 12, 2018

A Mysterious Russian Grey Hat Vigilante has patch

Hacking

In the interes
first reported
into people's
kind of digita

On a Russia
over 100,00(

- 2014 – A grey hat hacks thousands of Asus routers and planted text warnings about files that were left exposed and reminding users to patch.
- 2015 – A group of grey hats, ironically called the White team, releases a piece of malware that closes security holes in several models of Linux routers.
- 2017 – A grey hat releases a piece of malware that punishes people for not patching their IOT devices by either deleting firmware or bricking them.
- 2017 – A grey hat makes over 150,000 printers print a message to their owners about the dangers of leaving your printer exposed online.
- 2018 – Another grey hat renames thousands of MikroTik and Ubiquiti routers "HACKED" to scare their owners into updating them.

https://www.thesslstore.com/blog/mysterious-russian-grey-hat-vigilante-patched-over-100000-routers/

WHAT IS A CYBER VIGILANTE?

A REBEL WITH GOOD CAUSE

Vigilantism is "a social movement giving rise to premeditated acts of force -or threatened force -by autonomous citizens" Johnston (1996).

6 key elements of vigilantism, highlighted by Johnston:

- Planning, premeditation, and organization
- Private voluntary agency
- Autonomous citizenship
- The use or threatened use of force
- Reaction to crime and social deviance
- Personal and collective security

Vigilantes are practitioners of vigilantism. On the internet, these cyber vigilantes act outside of the criminal justice system to carry out missions of "good cause".

Cyber vigilantes usually act in response to a perceived and repercussive criminal act. There are many forms of cyber vigilantes including hacktivists, who hack for socio-political purposes.

In IoT, four cyber vigilantes created malwares to reduce vulnerable devices exploited by cyber criminals. All four malwares are explored.

Brickerbot	Silex	Wifatch	Hajime

Threat Events: Software Attacks (cont.)

a) Use of Malware

- **MALWARE** – a program that is **inserted into the victim system,** usually covertly, with the intent of:
  1) compromise the CIA of the victim's data, application(s) or the OS
  2) misuse the resources of the victim computer, or
  3) otherwise annoy or disrupt the victim

  (malware examples: *virus*, *worm*, *trojan*, *key-logger*, ...)

- **Common Malware Targets/Objectives**
  - steal credit card data, passwords, ...
  - destroy files, boot records, ...
  - store illegal music, movies, pirated software, ...

Threat Events: Software Attacks (cont.)

- **Malware Based on What it Does**
  - corruption of system or data files - virus & worms
  - turning the victim into a zombie - bot/botnets for DDoS
  - theft of information (logins, passwords, ...) - keyloggers & spyware
  - hiding of its presence - backdoors & rootkits

- **Malware Based on How It Spreads/Propagates**
  - carried/spread by 'carriers' + replicate = **virus**
  - spread over a network on their own + replicate = **worms**
  - use 'social engineering' to 'sneak in' = **trojans**

Different categories of malware ...

https://www.youtube.com/watch?v=n8mhzU0X2nQ

Threat Events: Software Attacks (cont.)

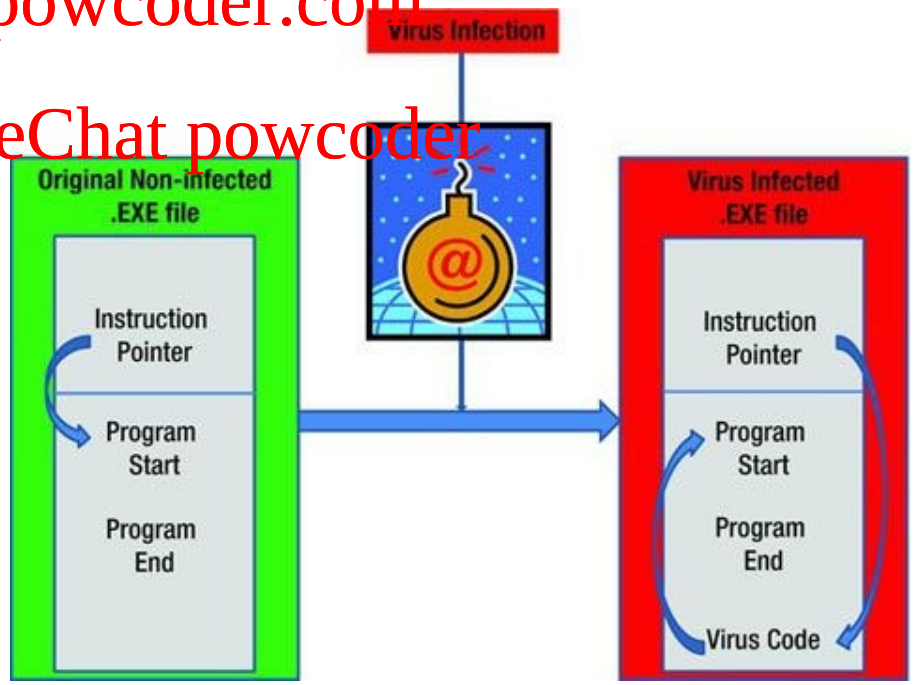
- **Malware Types**
  - Virus
  - Worm
  - Trojan horse
  - Logic Bomb
  - Rootkit
  - Information Stealer
  - Ransomware
  - Scareware
  - Spyware
  - Adware

Threat Events: Software Attacks (cont.)

- **VIRUS** – piece of software that 'infects' other host programs (executable) by modifying them

  - once a virus attaches to an executable, it can do anything that the executable is permitted to do (e.g., erase files & programs, change settings, etc.)

When viruses attach themselves to the executable files, they alter the instruction pointer of the executable programs in such a way that the virus code gets executed first before the actual executable code.



https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_7

Threat Events: Software Attacks (cont.)

- VIRUS

- **phases of virus lifetime**

1) propagation/infection phase - the virus places a copy of itself into other programs - each infected program will contain a clone of the virus which itself will enter a propagation/replication phase

2) dormant phase - the virus is idle and eventually gets activated by some event (date, presence of another program or file, ...) - not always present

3) triggering phase - the virus is activated to perform the function for which it was intended - again, it can be caused by a variety of system events (e.g., number of times that the virus has replicated)

4) execution phase - the malicious function is performed and can be
   - harmless, (e.g.) a message on the screen
   - harmful, (e.g.) destruction of programs or files

http://slideplayer.com/slide/4243337/

Virus Phases

dormant phase
- virus is idle
- will eventually be activated by some event
- not all viruses have this stage

triggering phase
- virus is activated to perform the function for which it was intended
- can be caused by a variety of system events

infects the system

propagation phase
- virus places a copy of itself into other programs or into certain system areas on the disk
- may not be identical to the propagating version
- each infected program will now contain a clone of the virus which will itself enter a propagation phase

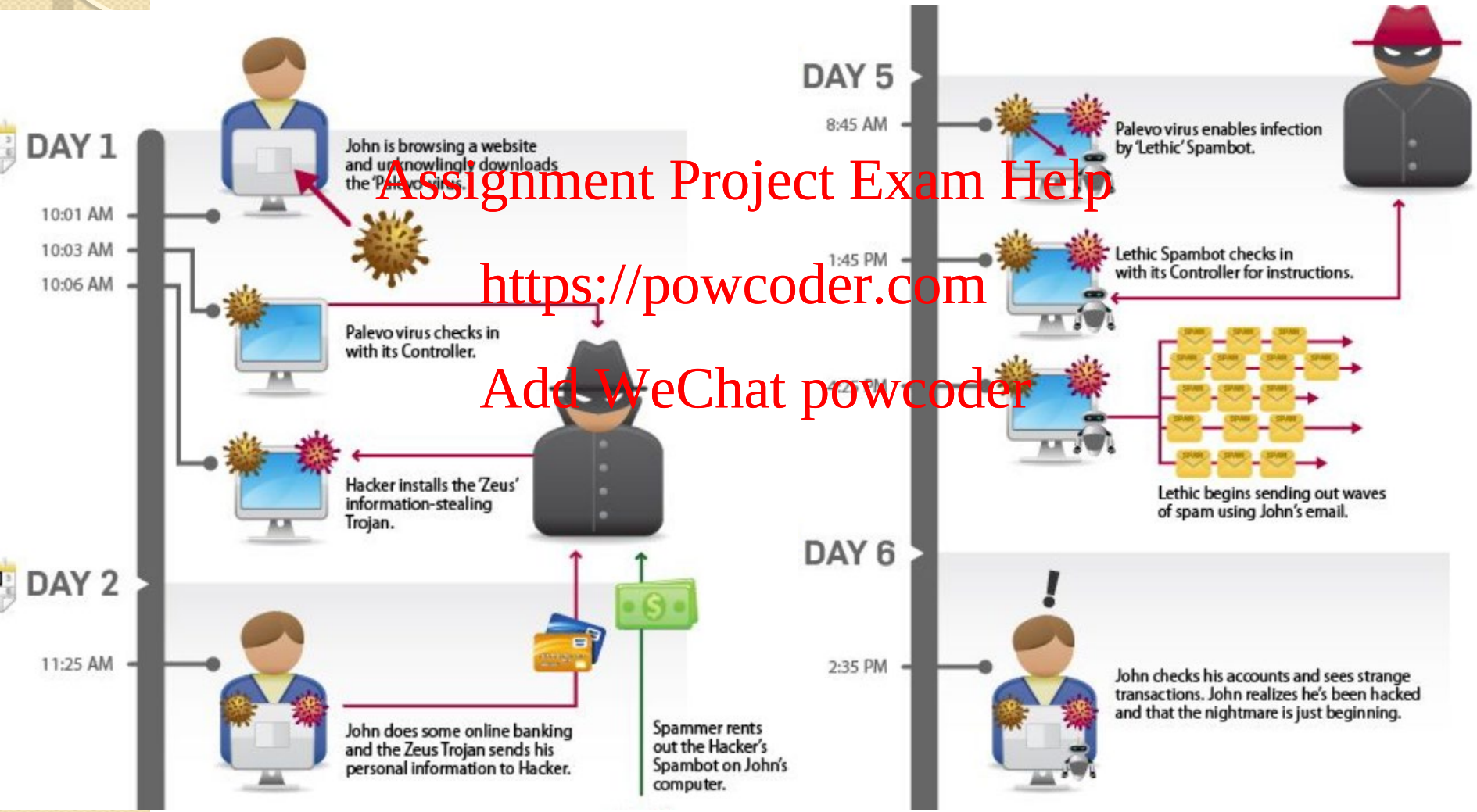
execution phase
- function is performed
- may be harmless or damaging

does the actual damage

✶ **IMPORTANT: viruses need '2 factors' to replicate -**
carrier = document or **host program**, and
user = to initiate the propagation/triggering

Threat Events: Software Attacks (cont.)

Example: 'many faces' virus infection



https://www.pinterest.es/pin/511862313880147170/

Threat Events: Software Attacks (cont.)

- **VIRUS** To infect the victim machine, virus must be executed! Different viruses rely on different tech. to be executed.

  - **classification of viruses by target / means of execution**

    a) **boot sector infector** - infects a master boot record and spreads when a system is booted from the disk containing the virus - nowadays rare

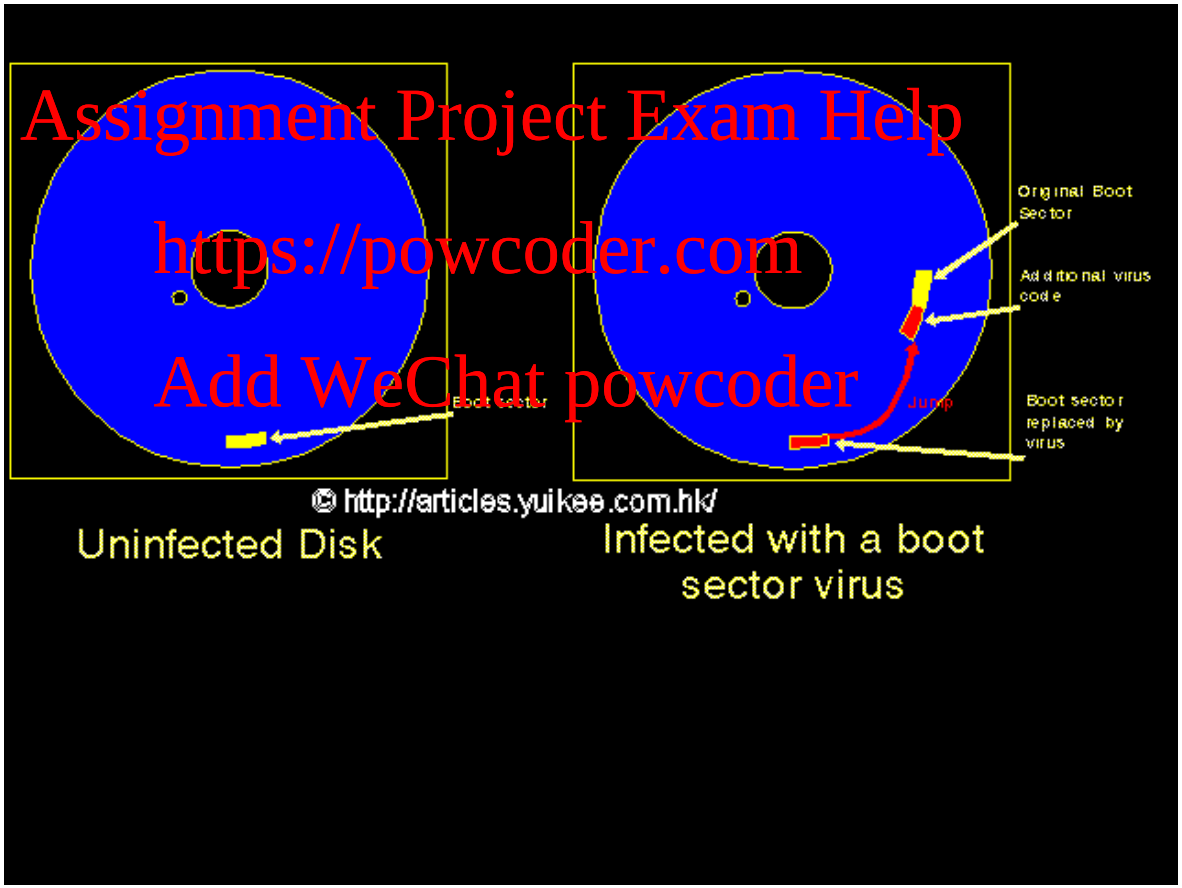
    b) **file infector** - infects executable files (.exe, .com)

    c) **macro virus** - infects files with macro or scripting code that are interpreted by an application - used to be very prevalent in early 2000-s
       - easily spread, as 'documents', not applications are commonly exchanged among users today

    d) **multipartite virus** - uses multiple 'attack vectors', e.g., both boot sector and executable files on hard drive - most difficult to eradicate

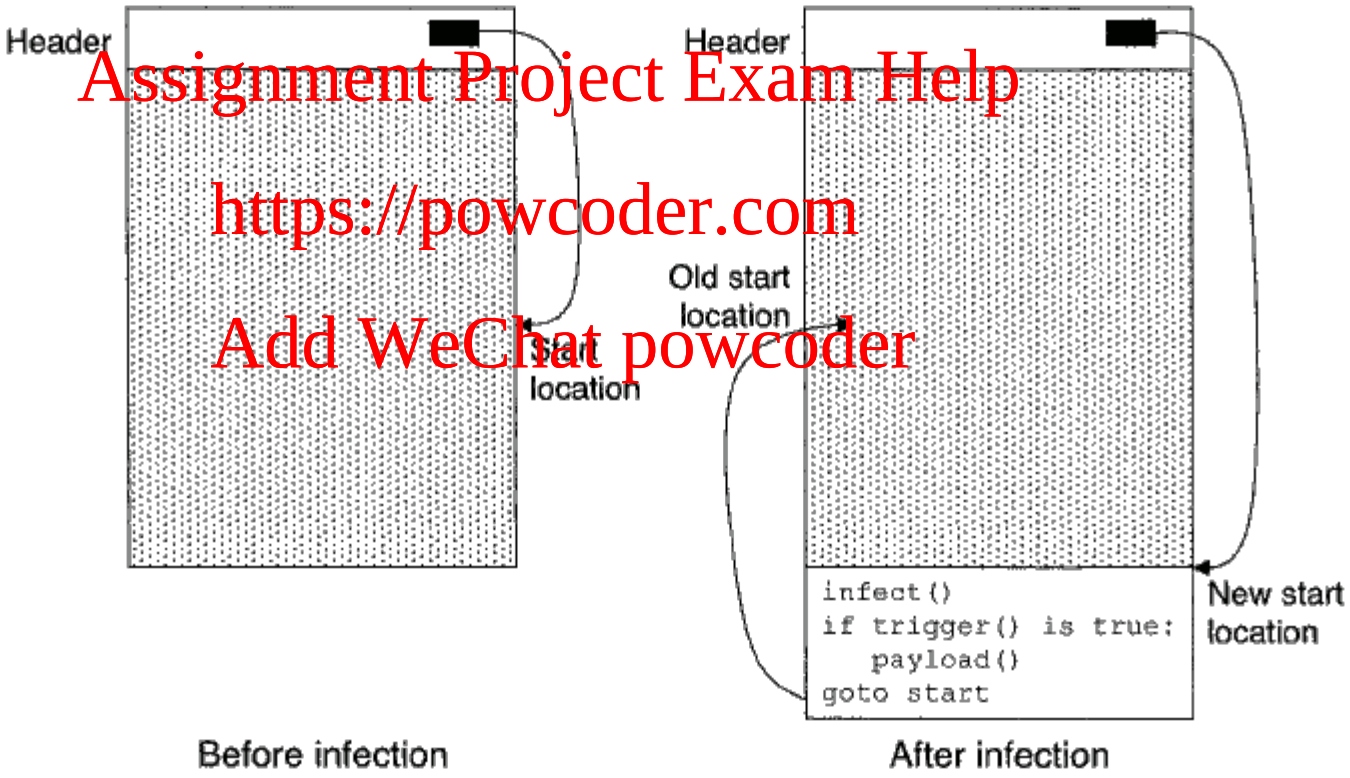
Threat Events: Software Attacks (cont.)

Boot Sector Virus



Threat Events: Software Attacks (cont.)

File Infector Virus [found in .exe, .com programs]



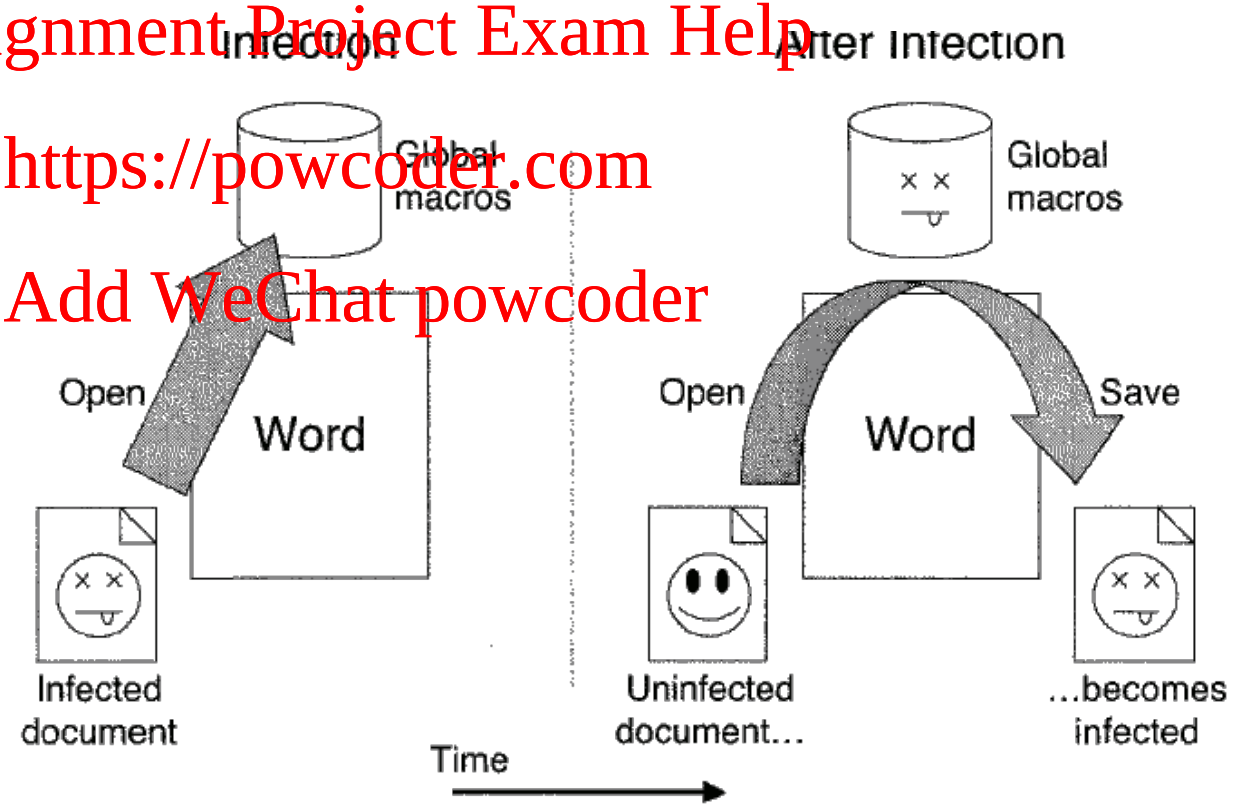
https://www.slideshare.net/hoangnamnguyen1694/ceh-v5-module-16-virus-and-worms

Threat Events: Software Attacks (cont.)

Macro Virus [found in .doc, .pdf files that get interpreted by MSWord and Acrobat]

macro - list of 'shortcut instructions' in a document

After a rush of macro viruses in the late part of the 20th century, productivity software developers made important changes to the macro development environment restricting ability of untrusted macros to run without user permission.



https://www.slideshare.net/lastlinesecurity/introduction-to-malware-part-1

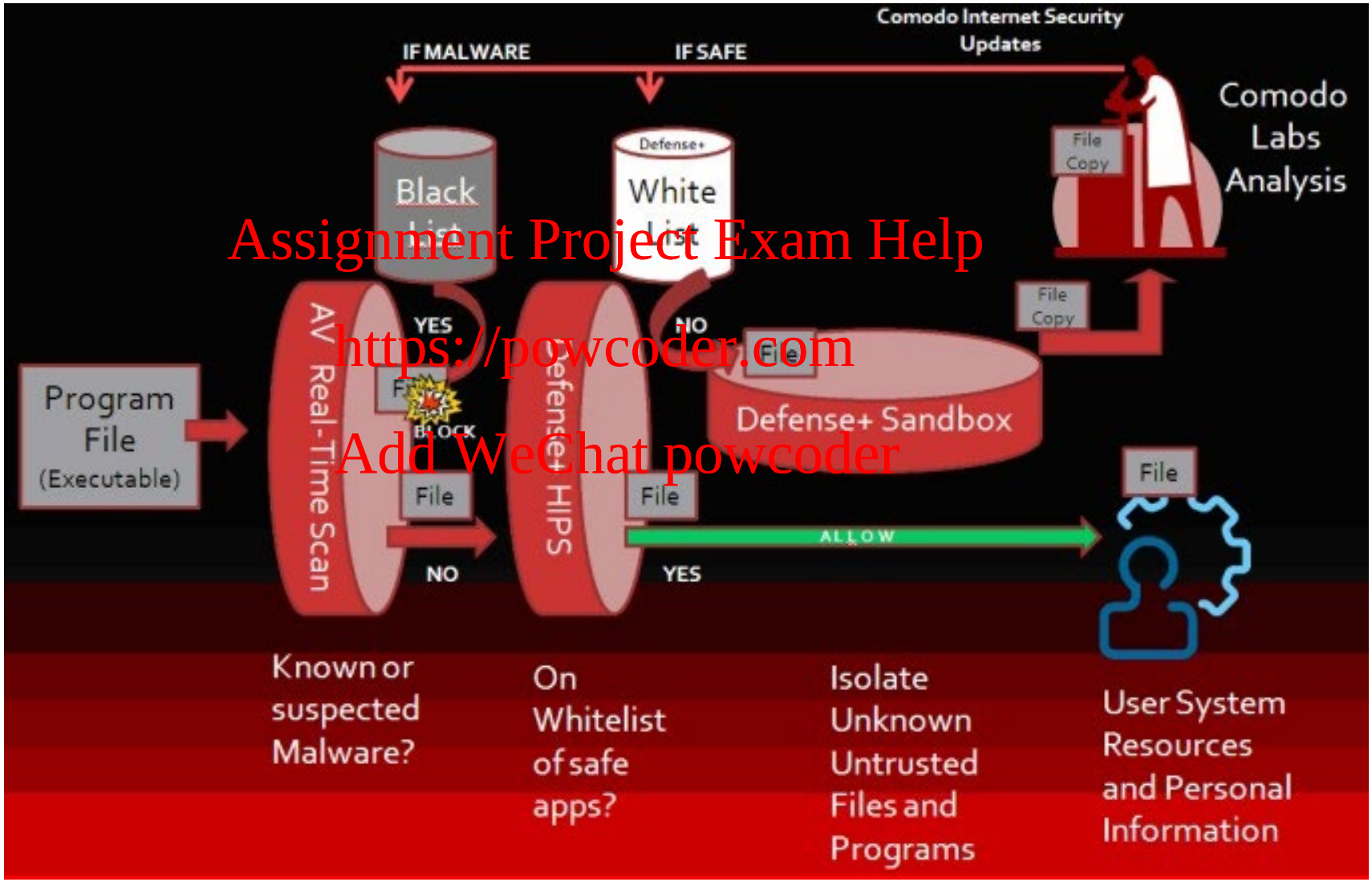
Threat Events: Software Attacks (cont.)

TYPES OF VIRUS CONTROLS. A computer virus may be categorized with one or more of the following four designations:

Boot sector infector	Master Boot Record (MBR) infector	File infector infector	Macro infector
•Boot sector viruses infect the boot record on hard disks, floppy disks, and theoretically also on CD's and DVD's. A boot sector virus does not need to be able to successfully boot the victims computer to infect it. Because of this, even non-bootable media can spread a boot sector virus.these viruses have become less common as floppy disks have become rarer.	•Master Boot Record (MBR) viruses are very similar to boot sector viruses, except that they infect the MBR (Master Boot Record) instead of the boot sector.	•File infector viruses infect files which contain executables code, such as .EXE and .COM files. Some file infectors are memory resident. This means that the virus will stay in memory and continue to infect other programs. Other file infector viruses only infect other files when they are executed.	•They infect certain types of data files, such as Word Documents, Excel Spreadsheets, PowerPoint Presentations, and Access Databases. Macro viruses typically use the Visual Basic macro language which is built into Microsoft Office applications.

How does ‘anti-virus’ work ??

All instances of anti-virus software are updated with latest ‘**signatures**’ of all known viruses.



https://antivirus.comodo.com/faq/how-antivirus-works.html