اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

Faculty of Computing
Fakulti Komputeran

Data & Network Security

Chapter 4 - Threats and Attacks

Outline

4.1 Attacker’s goals, capabilities, and motivations

4.2 Malware

4.3 Social engineering

4.4 Network specific threats and attack types

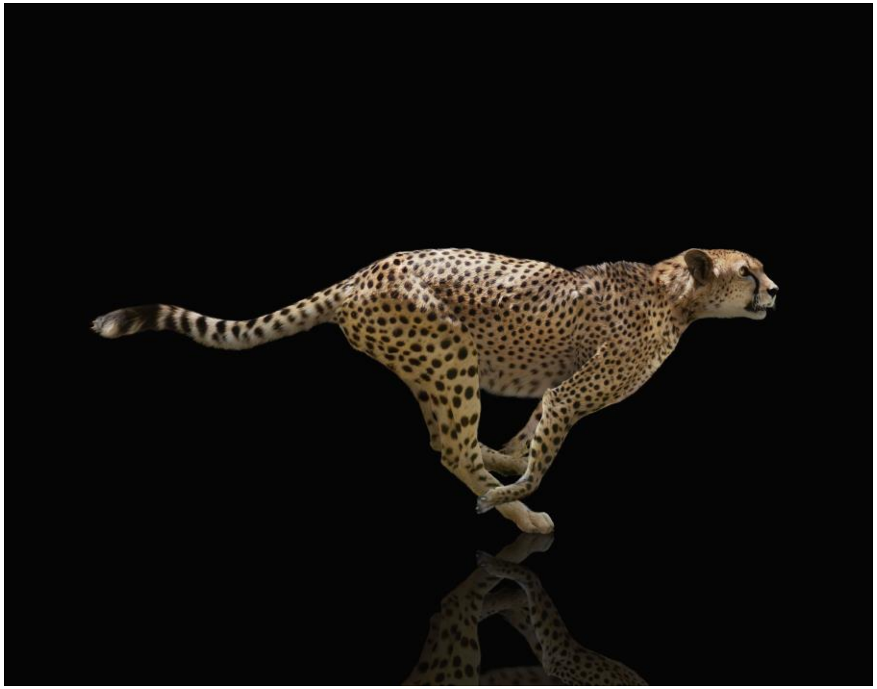
Learning Outcome

At the end of this chapter the students able to

- Understand the attacker’s goals, capabilities and motivations.
- Understand about the type of attackers.
- Analyze the type of a specific attack.
- Apply any solution for a specific attack.

Introduction

- Threats and attacks are two different concepts.
- In Computer Security, a threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.
- A threat can be either
  - ○ Intentional (an individual cracker or a criminal organization).
  - ○ Accidental (the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.



- Attack
  - ○ Act or action that exploits vulnerability (i.e., an identified weakness) in a controlled system.
  - ○ An action taken against a target to harm.

What is Cyberthreat?

A threat is any circumstance or event with the potential to adversely impact data or systems via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threats can be local, such as a **disgruntled employee**, or remote, such as an attacker in another geographical area.

© Rocheston 2023

A vulnerability is a **weakness in a system that can be exploited** to negatively impact confidentiality, integrity, and/or availability.

A software flaw vulnerability is caused by an unintended error in the design or coding of software.

No system is 100% secure: every system has vulnerabilities. At any given time, a system may not have any known software flaws, but security configuration issues and software feature misuse vulnerabilities are always present.

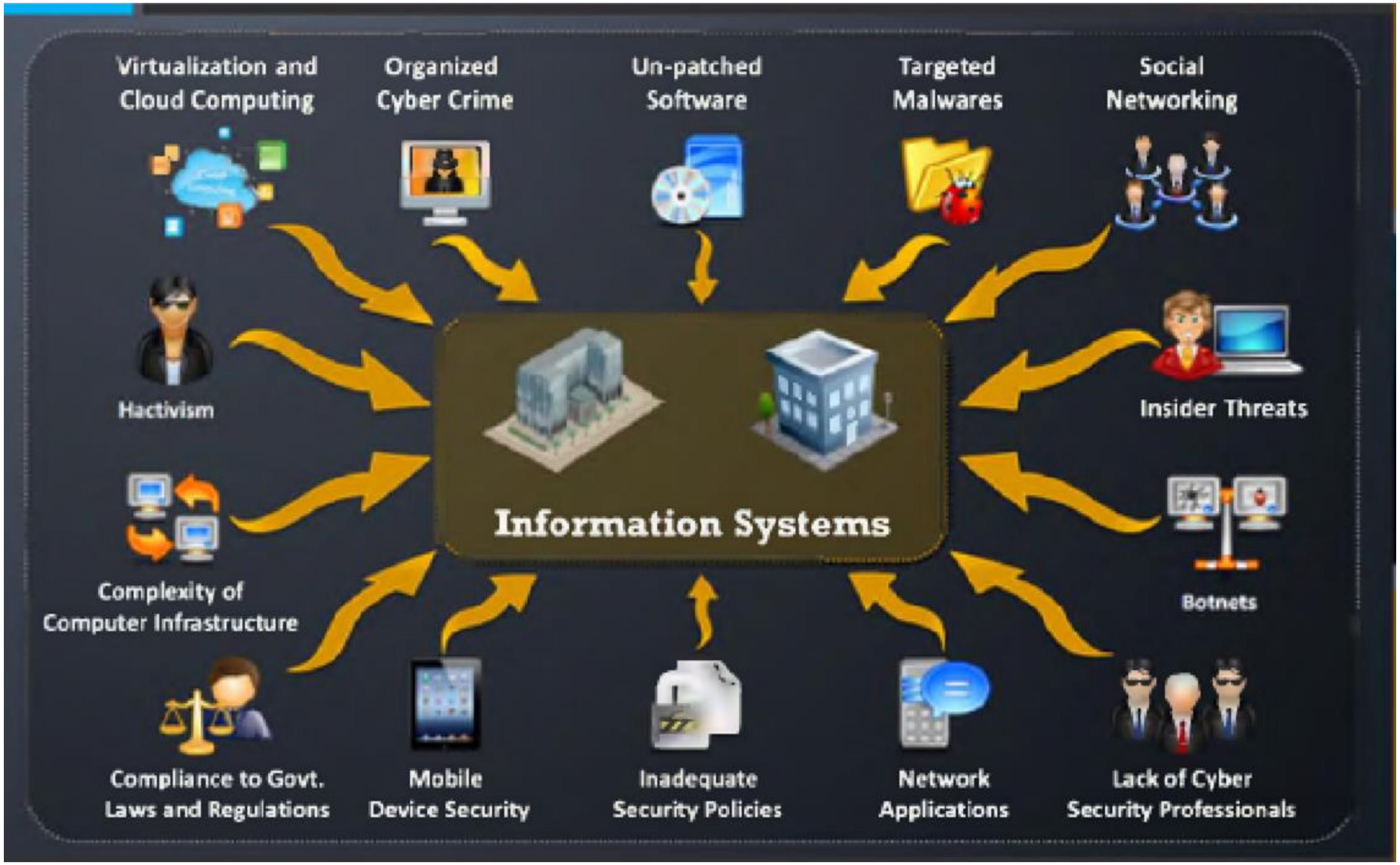
Vulnerabilities

© Rocheston 2023

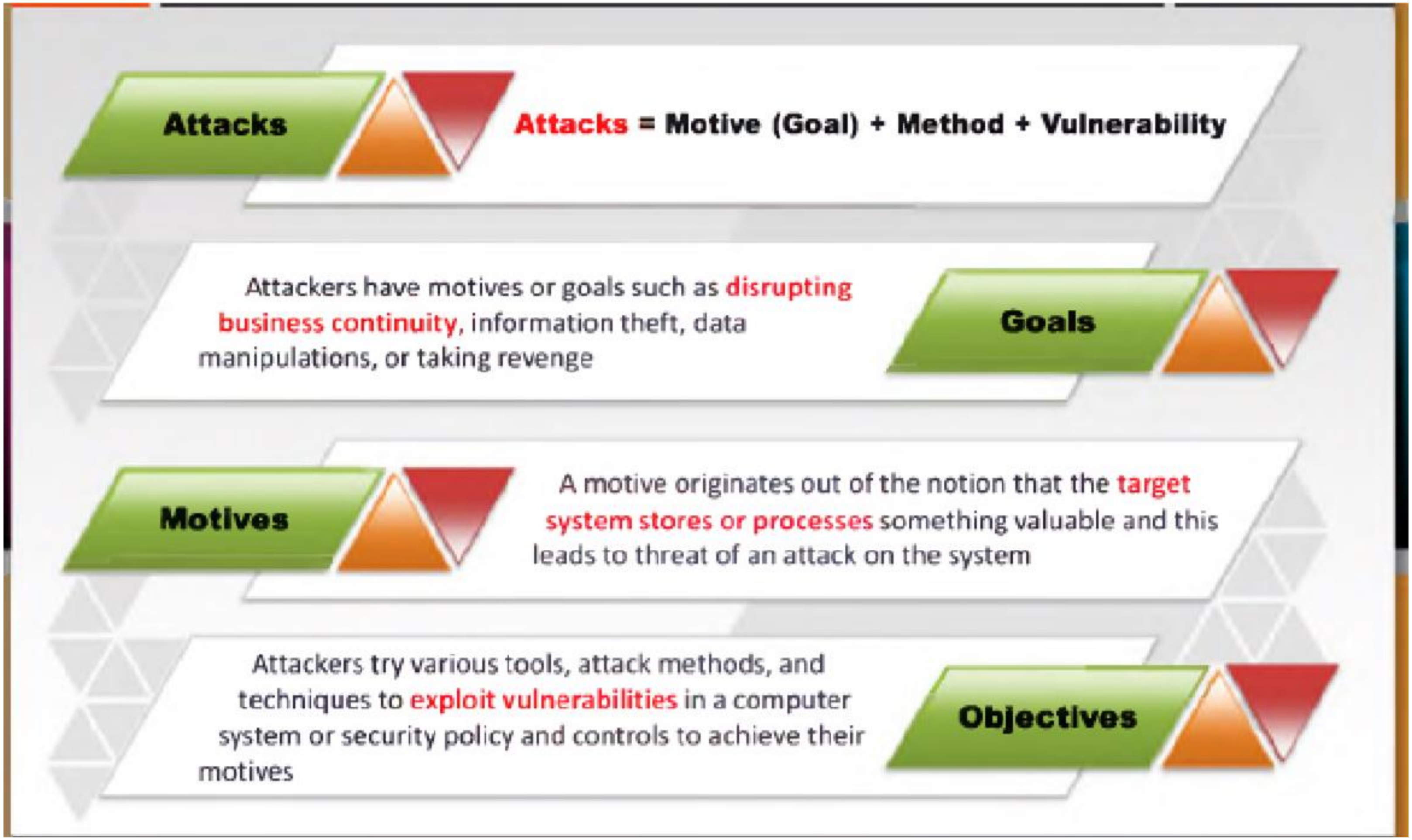
Sub-topic 4.1

Attacker’s goals, capabilities, and motivations

Attacker’s goals, capabilities, and motivations: Attack vector


Virtualization and Cloud Computing
Organized Cyber Crime
Un-patched Software
Targeted Malwares
Social Networking
Hactivism
Insider Threats
Information Systems
Complexity of Computer Infrastructure
Botnets
Compliance to Govt. Laws and Regulations
Mobile Device Security
Inadequate Security Policies
Network Applications
Lack of Cyber Security Professionals

Attacker's goals, capabilities, and motivations



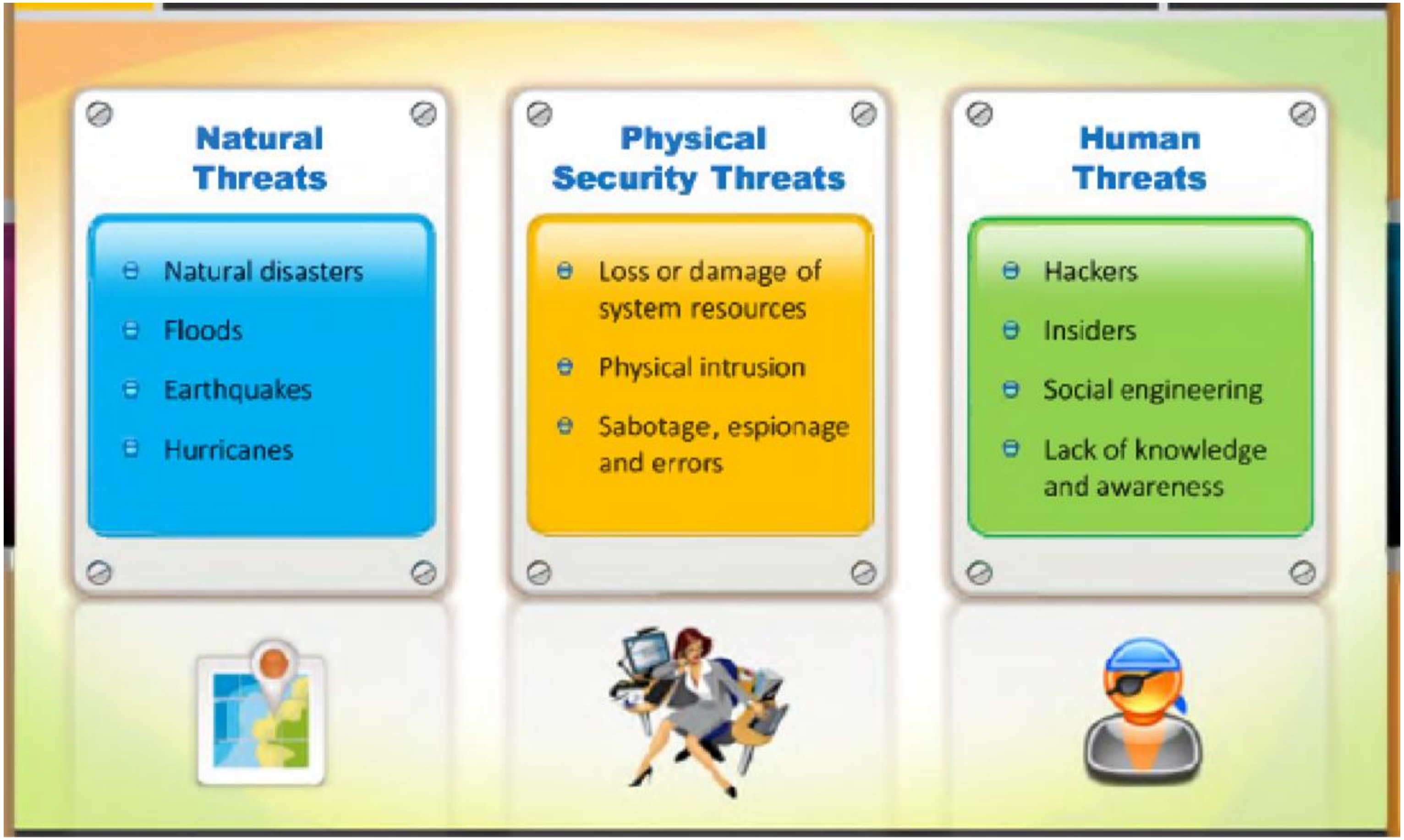
Attacks = Motive (Goal) + Method + Vulnerability

Attackers have motives or goals such as disrupting business continuity, information theft, data manipulations, or taking revenge

A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system

Attackers try various tools, attack methods, and techniques to exploit vulnerabilities in a computer system or security policy and controls to achieve their motives

Information security threats



Natural Threats

- Natural disasters
- Floods
- Earthquakes
- Hurricanes

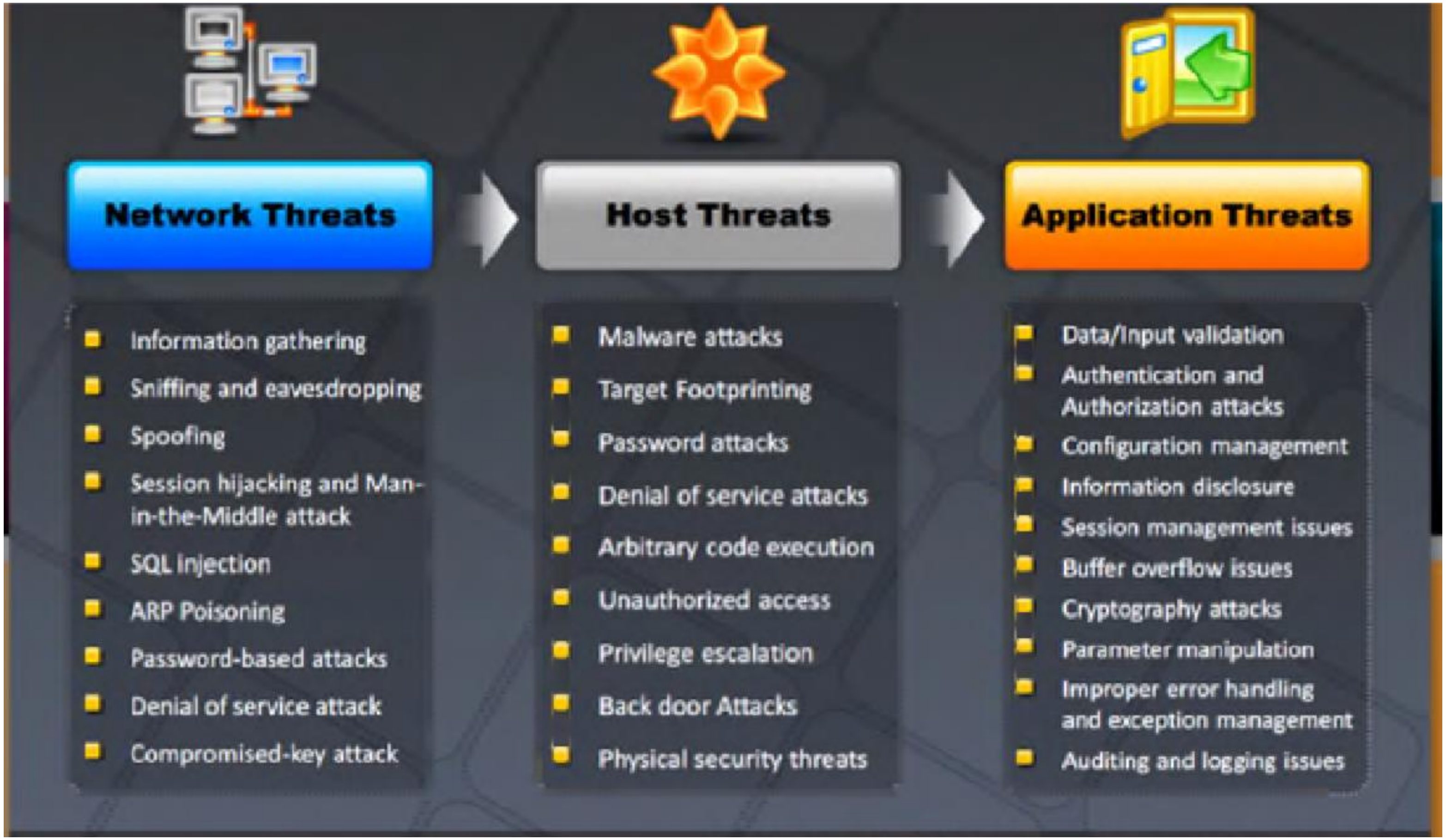
Physical Security Threats

- Loss or damage of system resources
- Physical intrusion
- Sabotage, espionage and errors

Human Threats

- Hackers
- Insiders
- Social engineering
- Lack of knowledge and awareness

Information security threats



Network Threats

- Information gathering
- Sniffing and eavesdropping
- Spoofing
- Session hijacking and Man-in-the-Middle attack
- SQL Injection
- ARP Poisoning
- Password-based attacks
- Denial of service attack
- Compromised-key attack

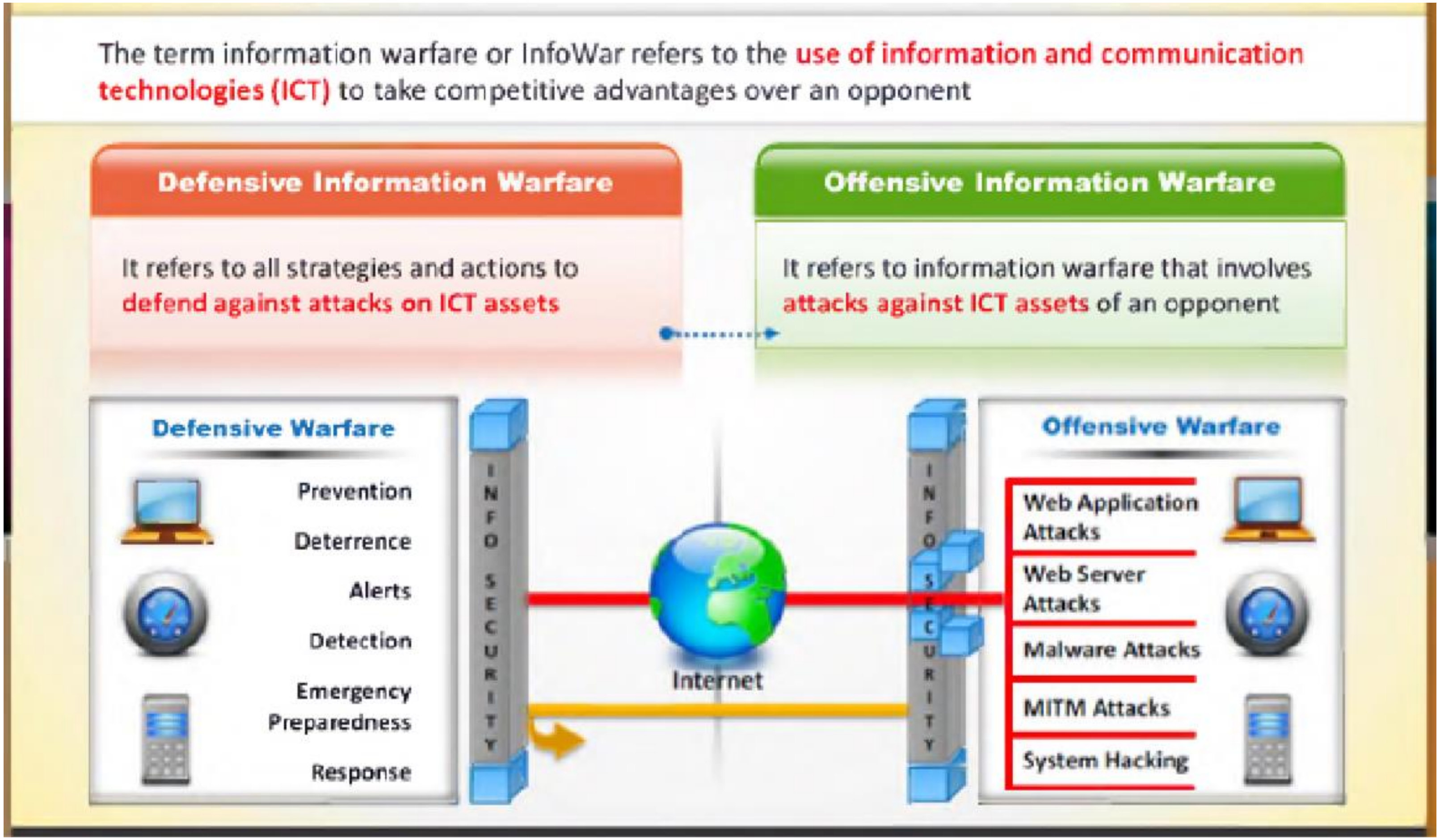
Host Threats

- Malware attacks
- Target Footprinting
- Password attacks
- Denial of service attacks
- Arbitrary code execution
- Unauthorized access
- Privilege escalation
- Back door Attacks
- Physical security threats

Application Threats

- Data/Input validation
- Authentication and Authorization attacks
- Configuration management
- Information disclosure
- Session management issues
- Buffer overflow issues
- Cryptography attacks
- Parameter manipulation
- Improper error handling and exception management
- Auditing and logging issues

Information warfare



The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) to take competitive advantages over an opponent

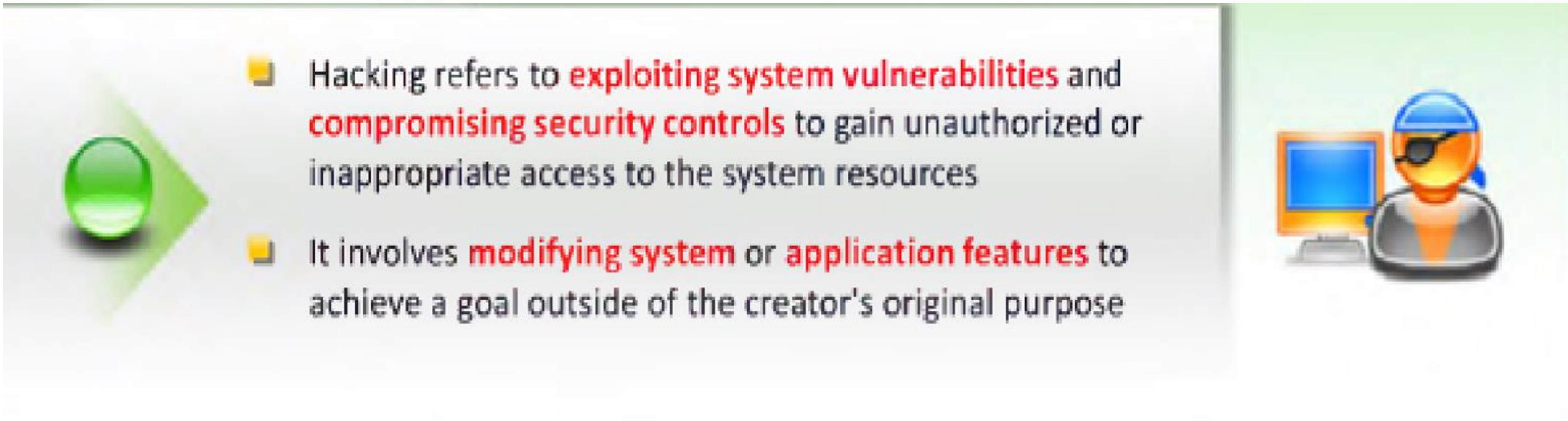
Defensive Information Warfare

It refers to all strategies and actions to defend against attacks on ICT assets

Offensive Information Warfare

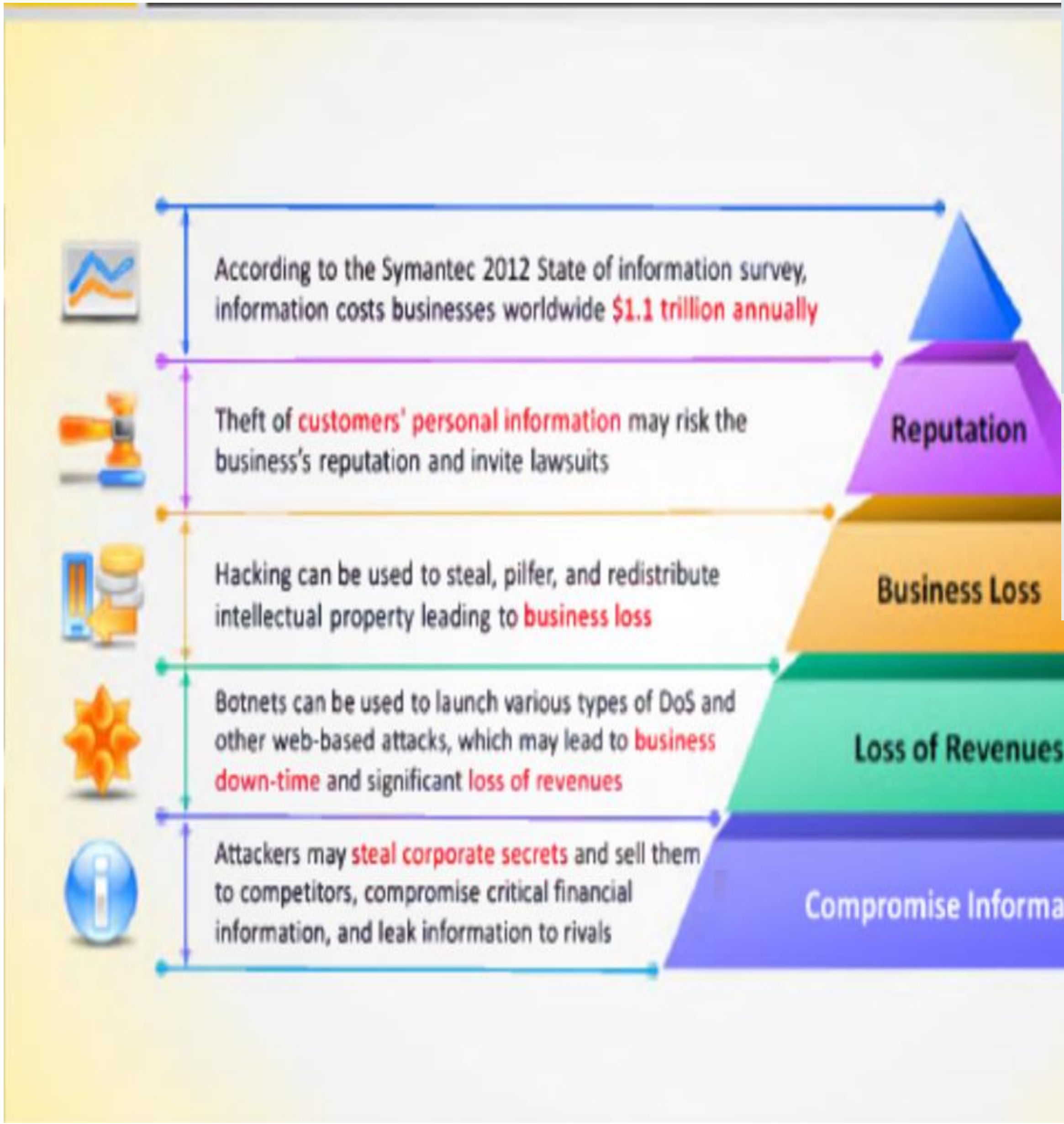
It refers to information warfare that involves attacks against ICT assets of an opponent

Hacking



- Hacking refers to **exploiting system vulnerabilities** and **compromising security controls** to gain unauthorized or inappropriate access to the system resources
- It involves **modifying system** or **application features** to achieve a goal outside of the creator's original purpose

Effects of hacking on business



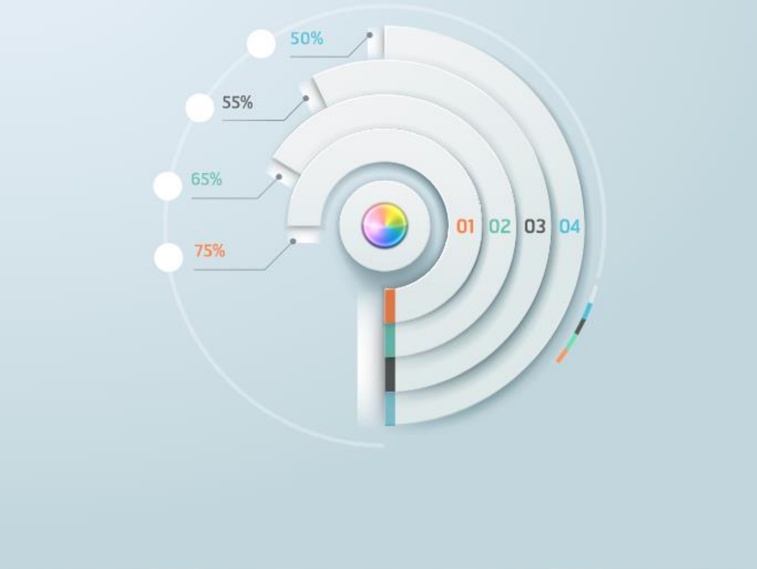
According to the Symantec 2012 State of information survey, information costs businesses worldwide $1.1 trillion annually

Theft of customers' personal information may risk the business's reputation and invite lawsuits

Hacking can be used to steal, pilfer, and redistribute intellectual property leading to business loss

Botnets can be used to launch various types of DoS and other web-based attacks, which may lead to business down-time and significant loss of revenues

Attackers may steal corporate secrets and sell them to competitors, compromise critical financial information, and leak information to rivals



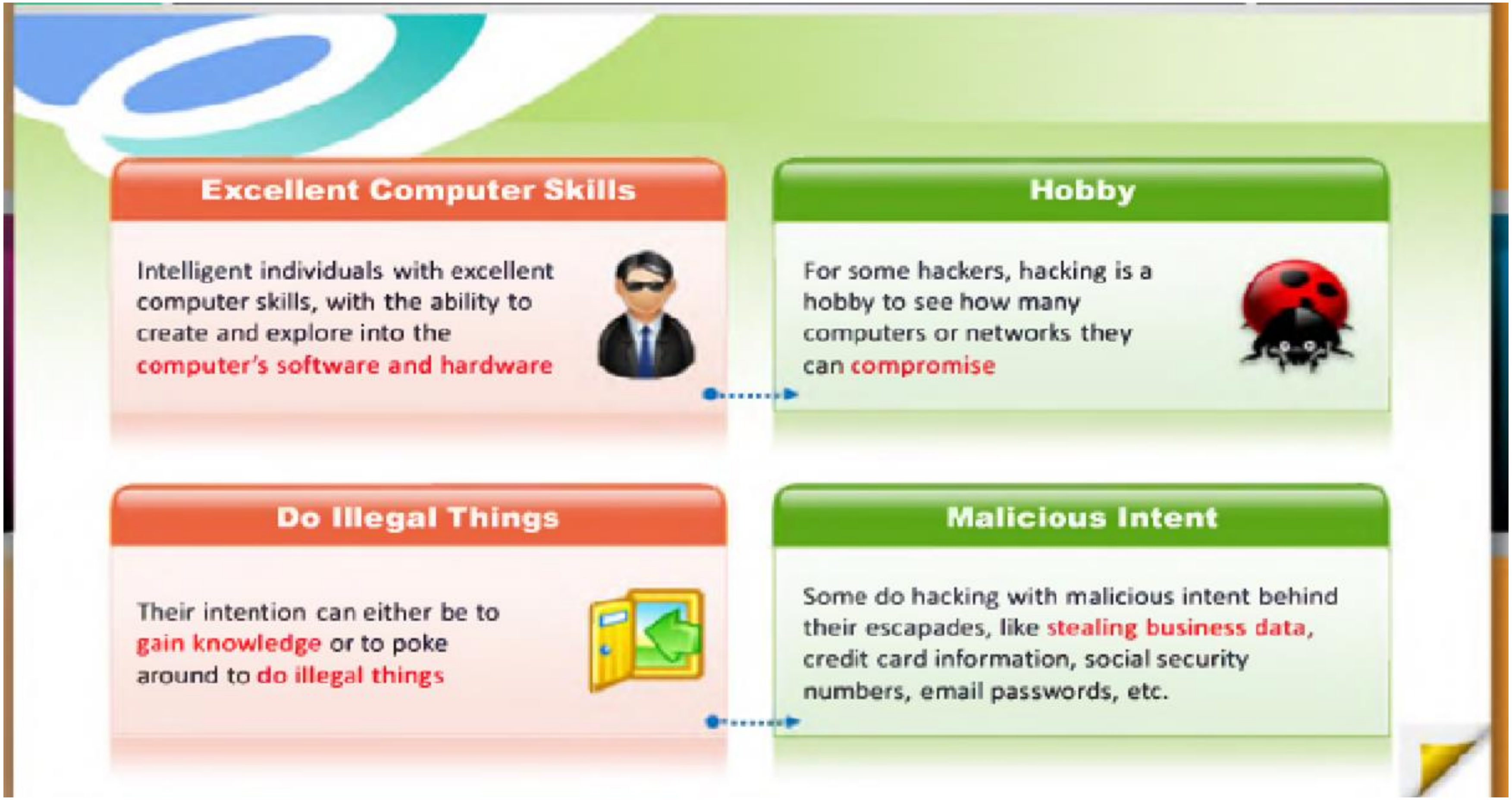
90% of businesses have been hit by a cyber security breach

"I've yet to come across a network that hasn't been breached."

-Shawn Henry
Former Head of Cybersecurity investigations for the FBI

© Rocheston 2023

Who is hacker?



Excellent Computer Skills

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

Hobby

For some hackers, hacking is a hobby to see how many computers or networks they can compromise

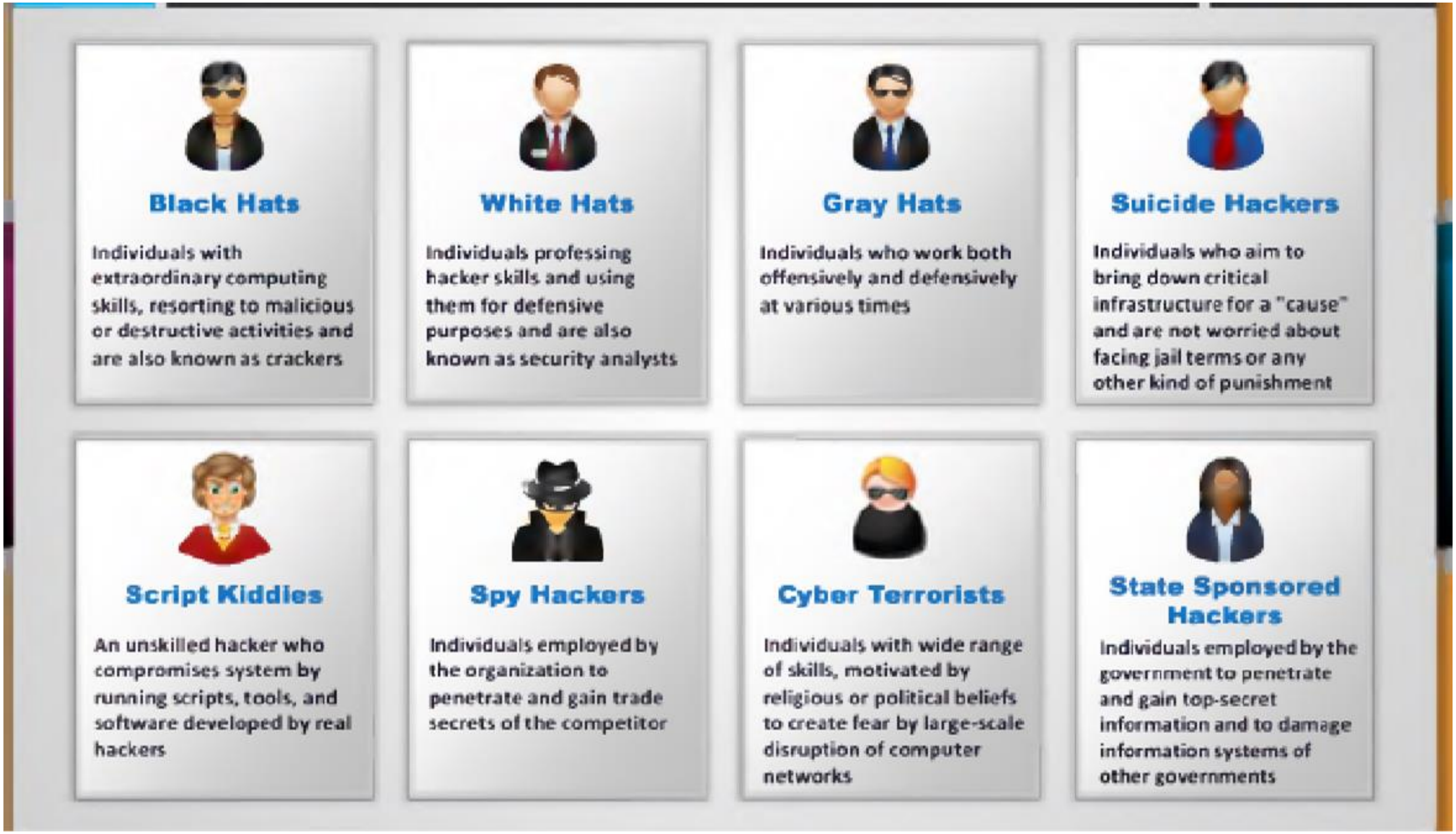
Do Illegal Things

Their intention can either be to gain knowledge or to poke around to do illegal things

Malicious Intent

Some do hacking with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, email passwords, etc.

Hackers



Black Hats

Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers

White Hats

Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts

Gray Hats

Individuals who work both offensively and defensively at various times

Suicide Hackers

Individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

Script Kiddies

An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers

Spy Hackers

Individuals employed by the organization to penetrate and gain trade secrets of the competitor

Cyber Terrorists

Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks

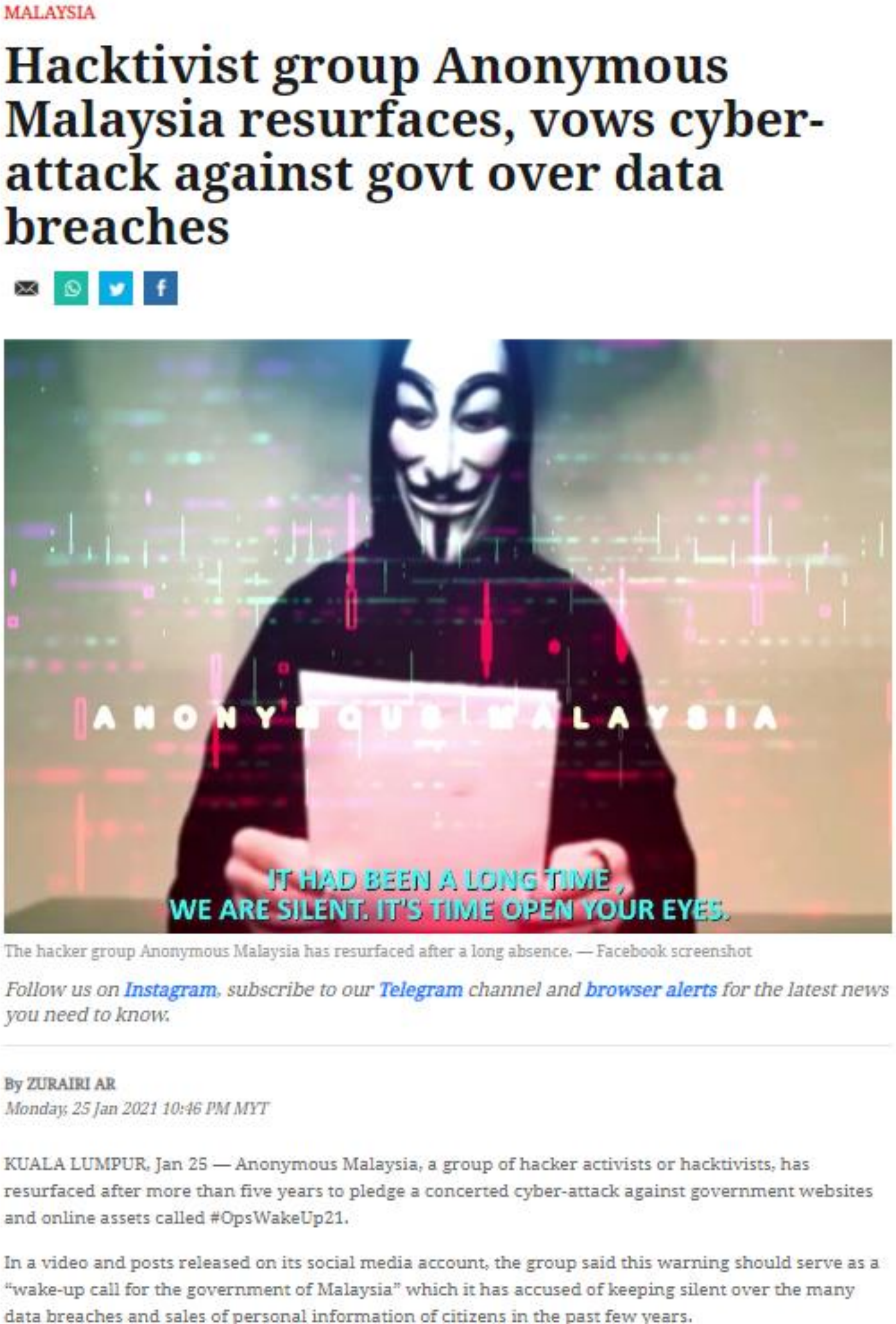
State Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments

- Hacktivism is an act of **promoting a political agenda** by hacking, especially by defacing or disabling websites
- It **thrives in the environment** where information is easily accessible
- Aims at **sending a message** through their hacking activities and gaining visibility for their cause
- Common targets include **government agencies, multinational corporations,** or any other entity perceived as bad or wrong by these groups or individuals
- It remains a fact, however, that **gaining unauthorized access** is a crime, no matter what the intention is
- Hacktivism is motivated by revenge, political or social reasons, ideology, vandalism, protest, and a desire to **humiliate victims**

Hacktivism

https://www.malaymail.com/news/malaysia/2021/01/25/hacktivist-group-anonymous-malaysia-resurfaces-vows-cyber-attack-against-go/1943943



MALAYSIA

Hacktivist group Anonymous Malaysia resurfaces, vows cyber-attack against govt over data breaches

The hacker group Anonymous Malaysia has resurfaced after a long absence. — Facebook screenshot

Follow us on ***Instagram****, subscribe to our* ***Telegram*** *channel and* ***browser alerts*** *for the latest news you need to know.*

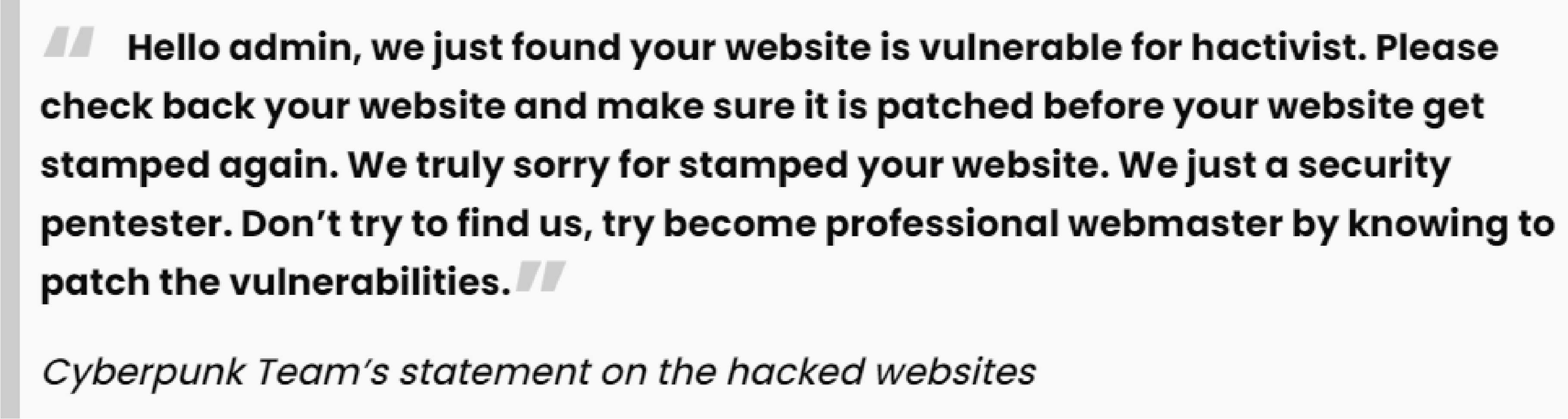
By ZURAIRI AR

Monday, 25 Jan 2021 10:46 PM MYT

KUALA LUMPUR, Jan 25 — Anonymous Malaysia, a group of hacker activists or hacktivists, has resurfaced after more than five years to pledge a concerted cyber-attack against government websites and online assets called #OpsWakeUp21.

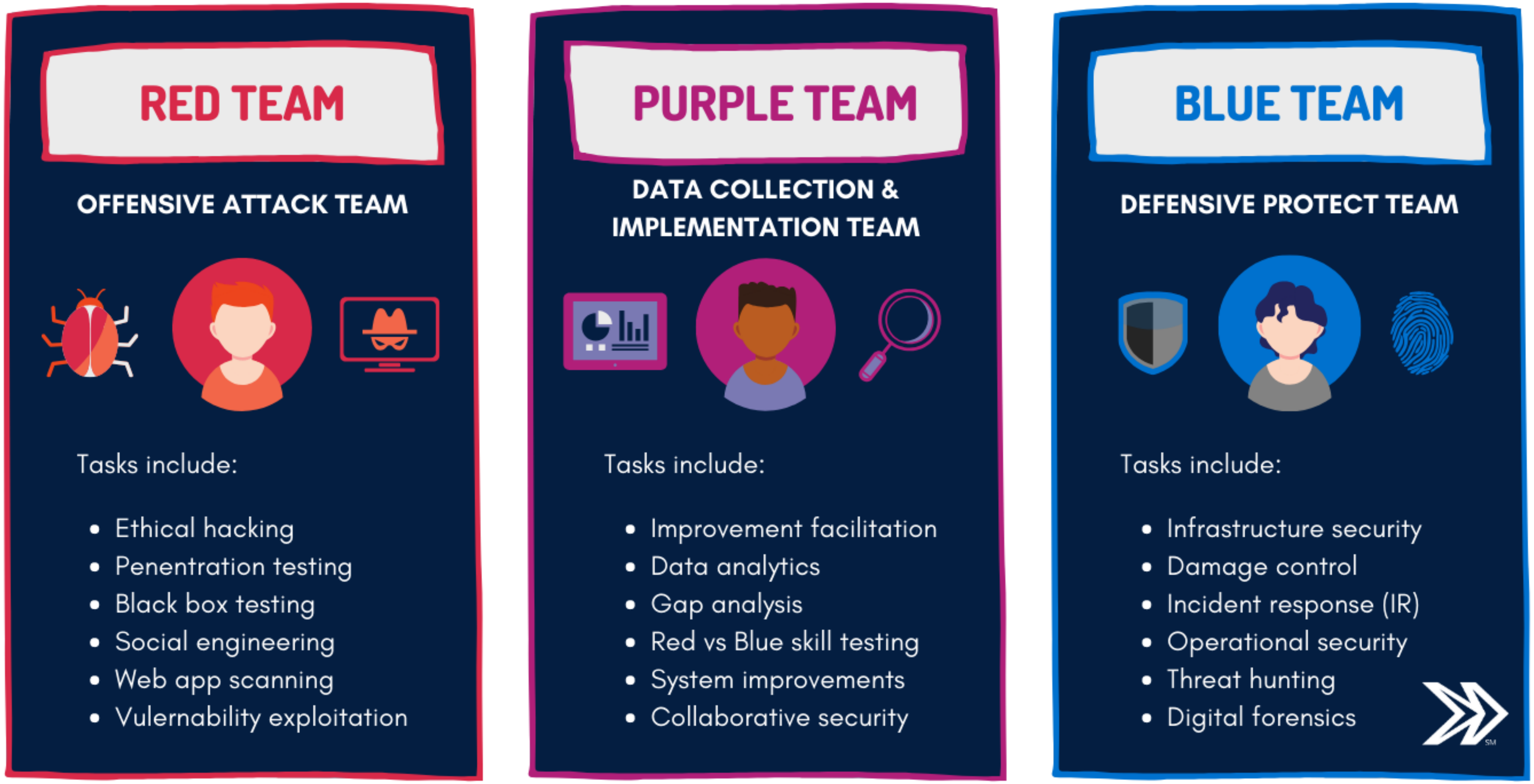
In a video and posts released on its social media account, the group said this warning should serve as a "wake-up call for the government of Malaysia" which it has accused of keeping silent over the many data breaches and sales of personal information of citizens in the past few years.

Hacktivism



> “Hello admin, we just found your website is vulnerable for hactivist. Please check back your website and make sure it is patched before your website get stamped again. We truly sorry for stamped your website. We just a security pentester. Don’t try to find us, try become professional webmaster by knowing to patch the vulnerabilities.”
>
> *Cyberpunk Team’s statement on the hacked websites*

https://www.therakyatpost.com/news/malaysia/2021/02/01/anonymousmy-claims-they-hacked-into-5-government-websites-to-prove-how-vulnerable-the-websites-are/



RED TEAM

OFFENSIVE ATTACK TEAM

Tasks include:

- Ethical hacking
- Penentration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulnerability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM

Tasks include:

- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics

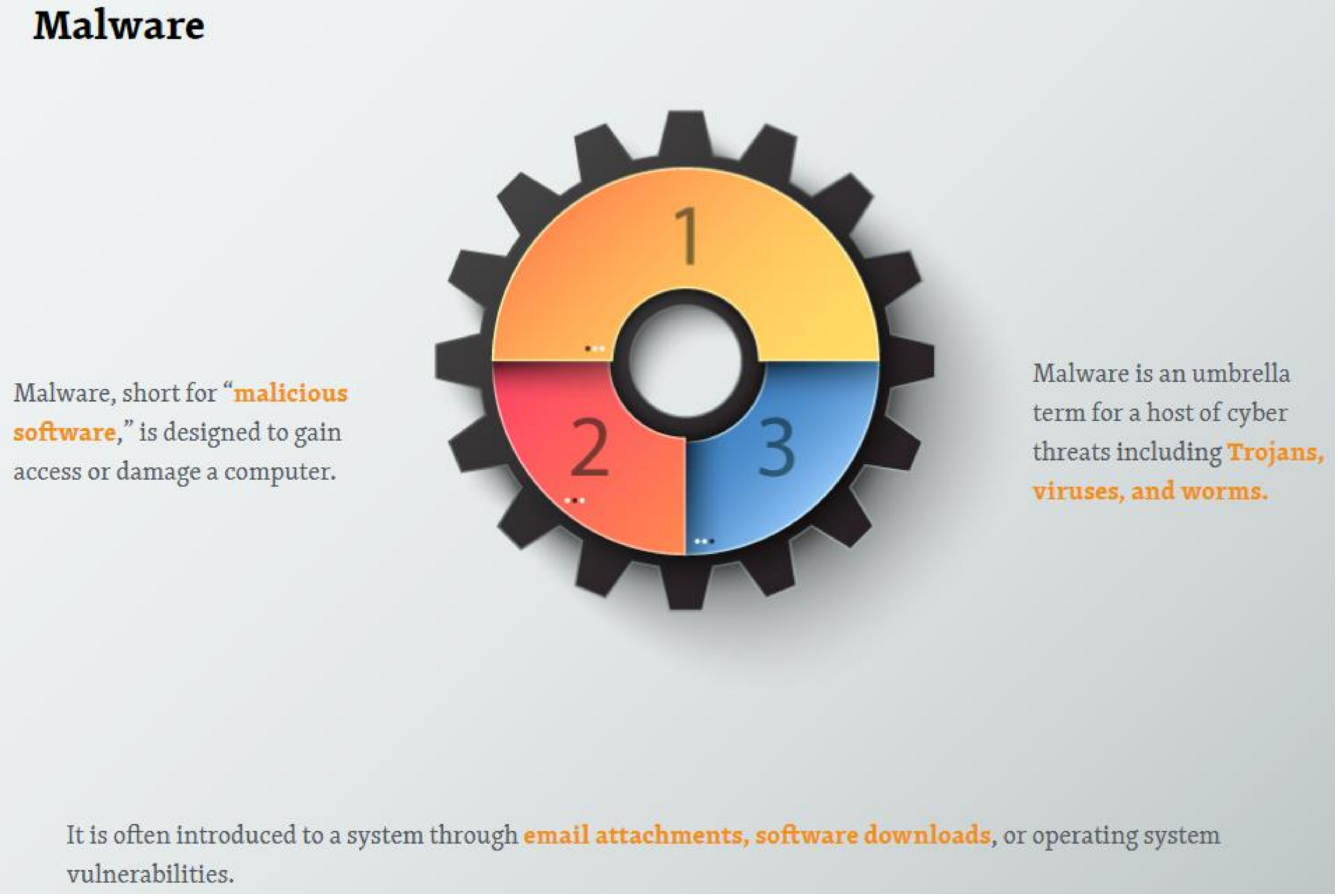
What does a red team do in cyber security?

Definitions: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.

Source (2023): https://gomindsight.com/insights/blog/red-team-vs-blue-team/ and https://csrc.nist.gov Red Team - Glossary

Sub-topic 4.2

Malware



Malware

Malware, short for "**malicious software**," is designed to gain access or damage a computer.

Malware is an umbrella term for a host of cyber threats including **Trojans, viruses, and worms.**

It is often introduced to a system through **email attachments, software downloads**, or operating system vulnerabilities.

© Rocheston 2023

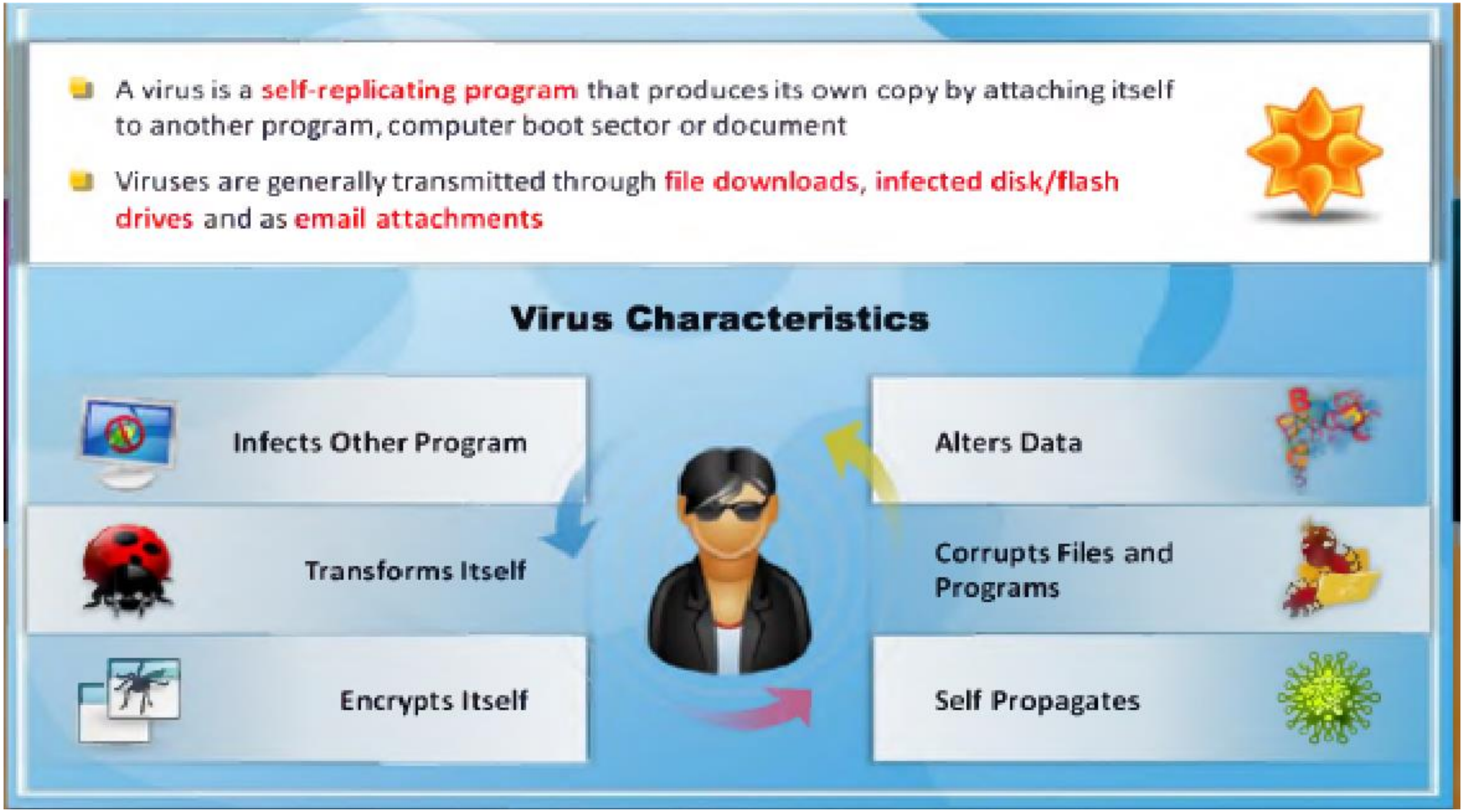
- There are several types of malware that can be differentiated based on the behaviour and affection of the victims.
  - ○ Viruses
  - ○ Worms
  - ○ Spyware
  - ○ Botnets
  - ○ Trojan horses
  - ○ Rootkits

Pharming
Eavesdropping
Ransomware
Viruses
Spam
Trojans
Identity Spoofing
Worms
Denial of Service
Phishing
10 COMMON CYBERATTACKS

Type of Malware

© Rocheston 2023

Virus

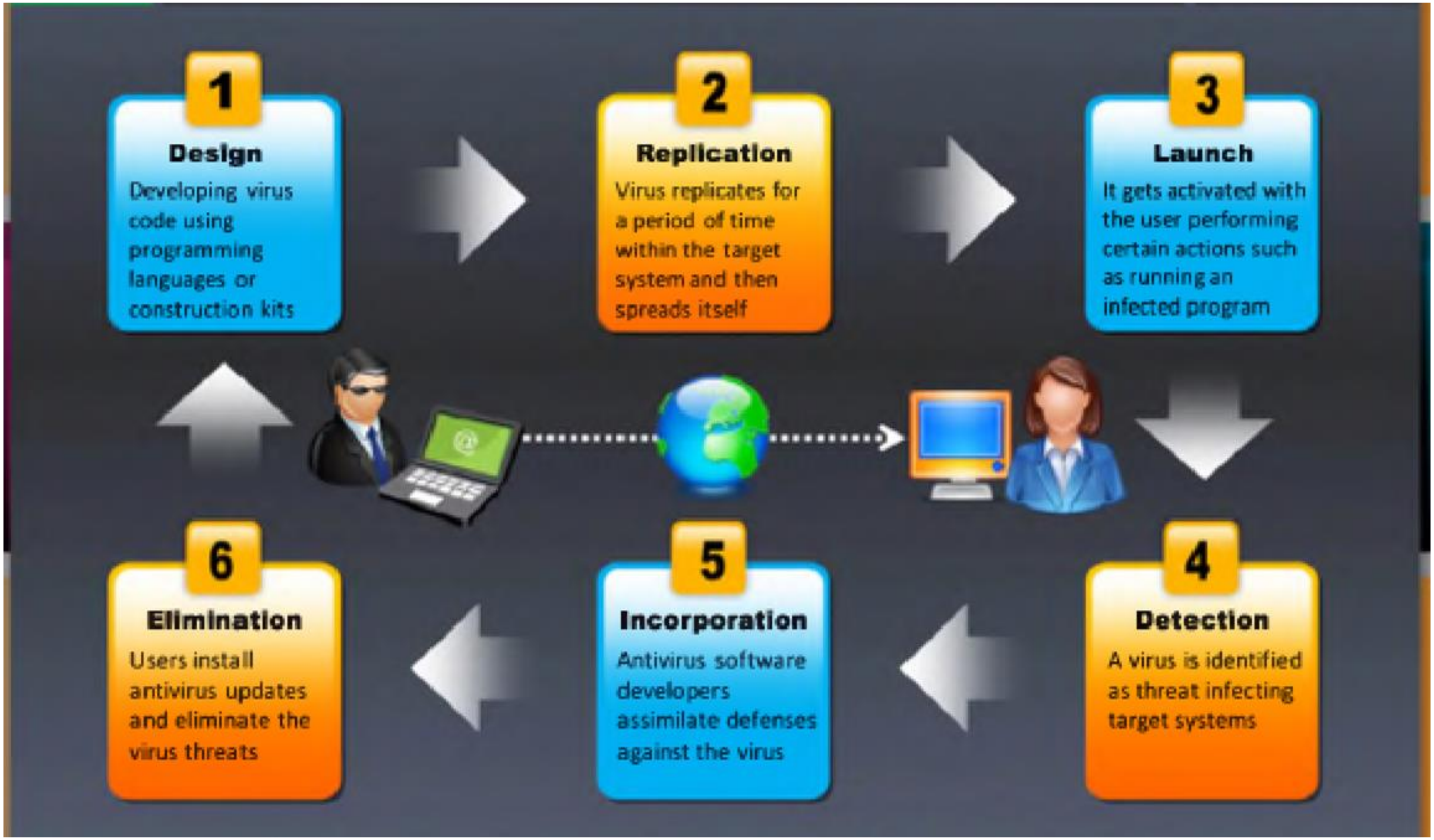


- A virus is a **self-replicating program** that produces its own copy by attaching itself to another program, computer boot sector or document
- Viruses are generally transmitted through **file downloads, infected disk/flash drives** and as **email attachments**

Virus Characteristics

- Infects Other Program
- Transforms Itself
- Encrypts Itself
- Alters Data
- Corrupts Files and Programs
- Self Propagates

Stages in life of a virus



1 **Design**
Developing virus code using programming languages or construction kits

2 **Replication**
Virus replicates for a period of time within the target system and then spreads itself

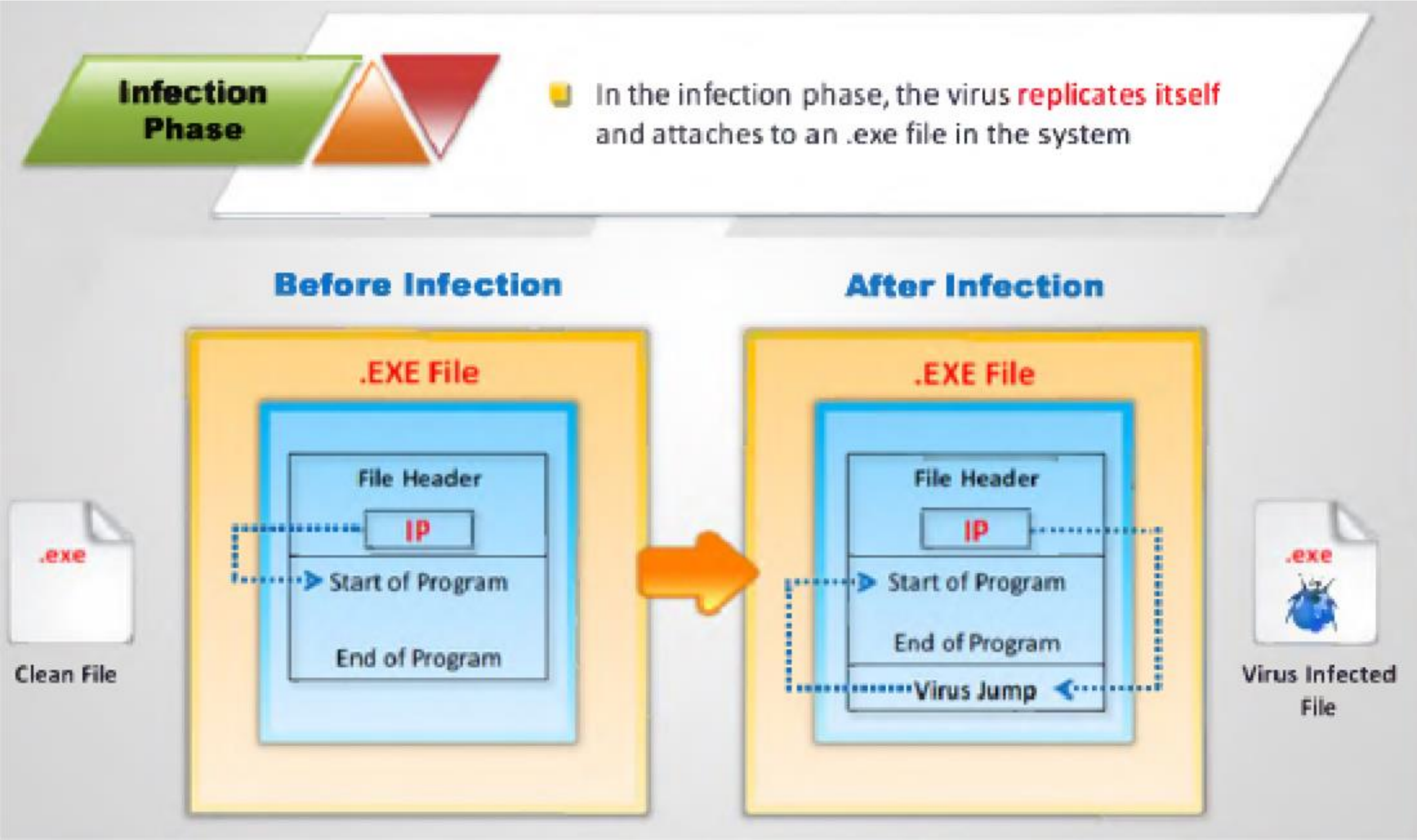
3 **Launch**
It gets activated with the user performing certain actions such as running an infected program

4 **Detection**
A virus is identified as threat infecting target systems

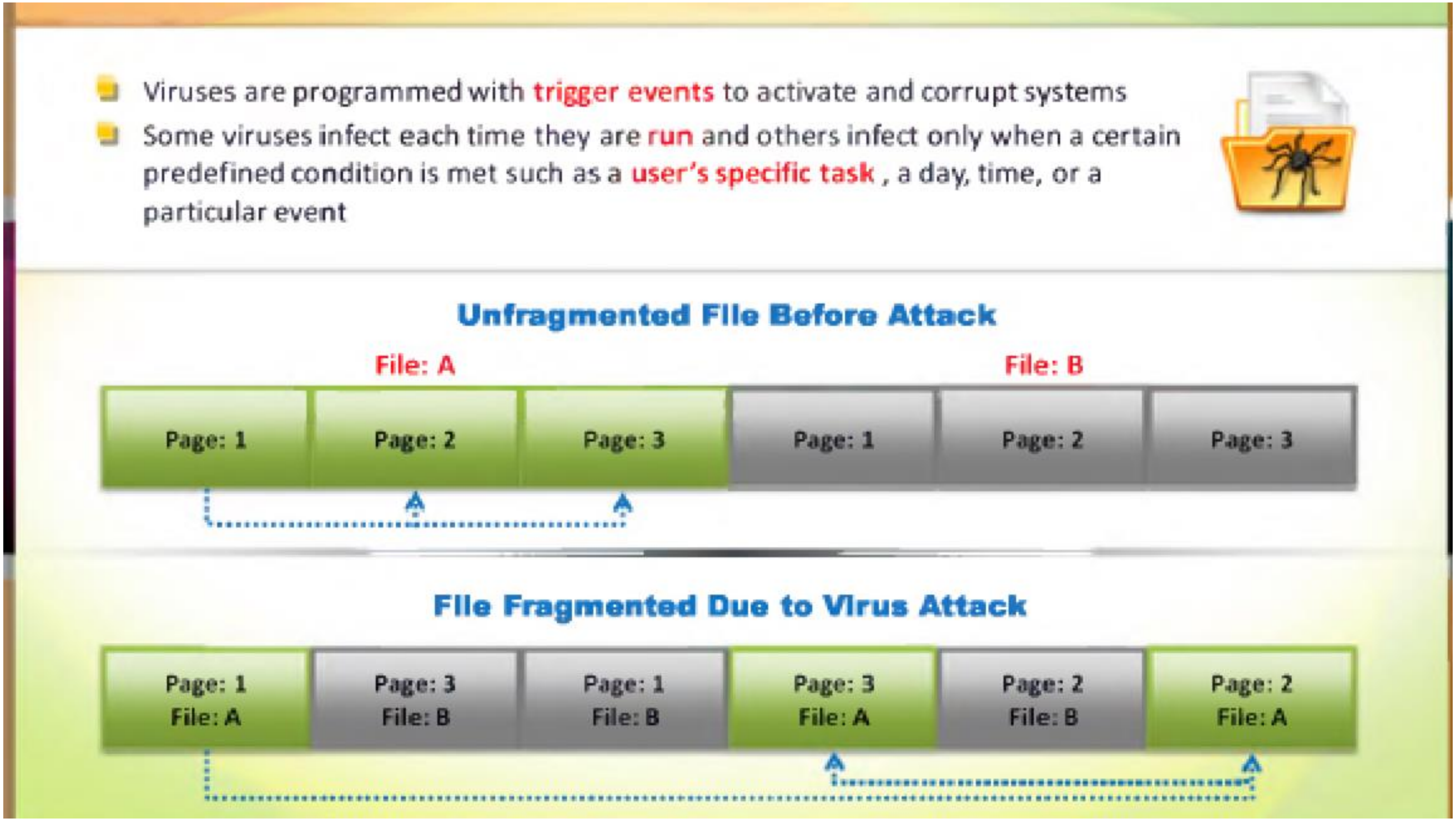
5 **Incorporation**
Antivirus software developers assimilate defenses against the virus

6 **Elimination**
Users install antivirus updates and eliminate the virus threats

Working of virus: Infection phase



Working of virus: Attack phase



- Viruses are programmed with trigger events to activate and corrupt systems
- Some viruses infect each time they are run and others infect only when a certain predefined condition is met such as a user's specific task , a day, time, or a particular event

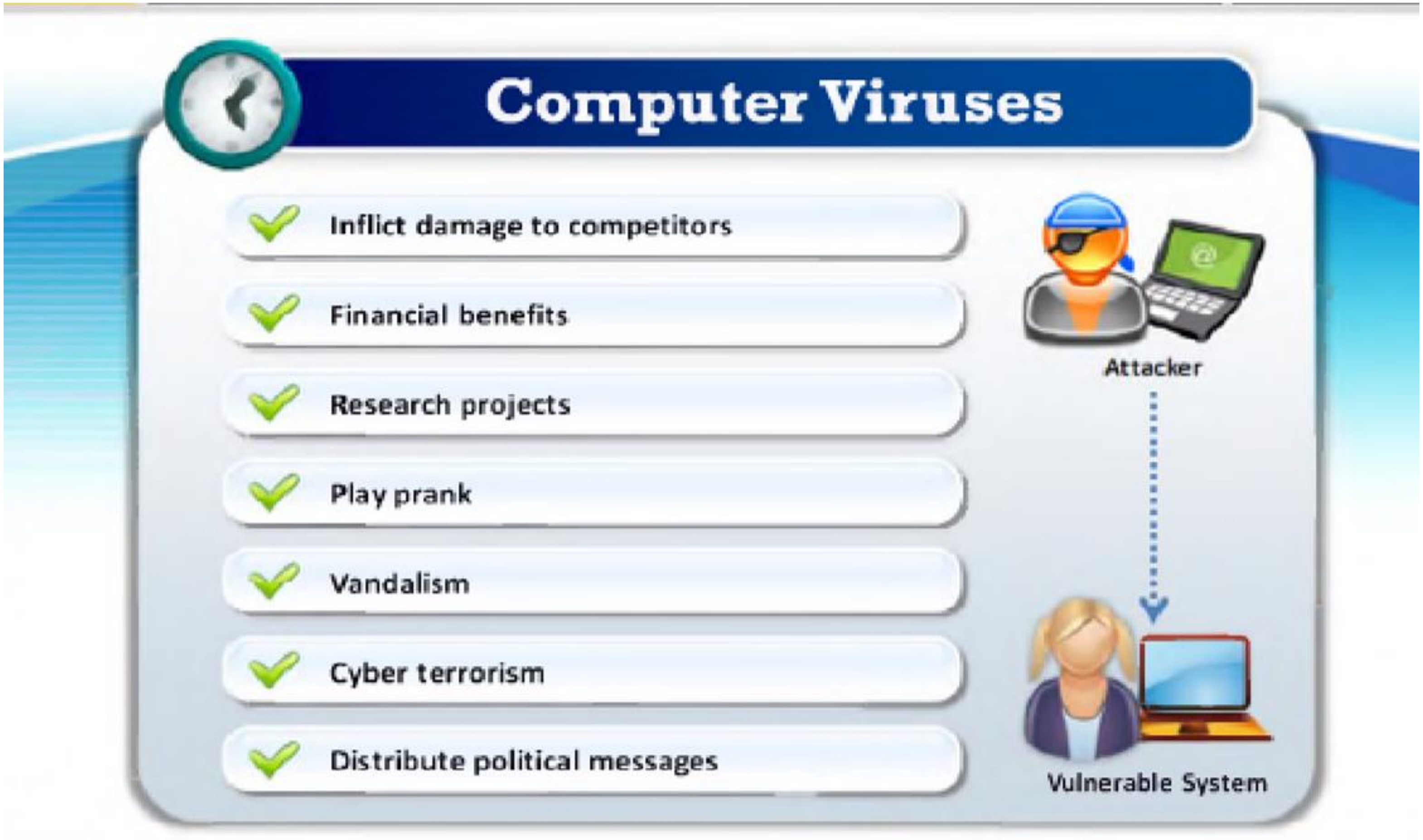
Unfragmented File Before Attack

File: A			File: B		
Page: 1	Page: 2	Page: 3	Page: 1	Page: 2	Page: 3

File Fragmented Due to Virus Attack

Page: 1 File: A	Page: 3 File: B	Page: 1 File: B	Page: 3 File: A	Page: 2 File: B	Page: 2 File: A

Reason for creating virus



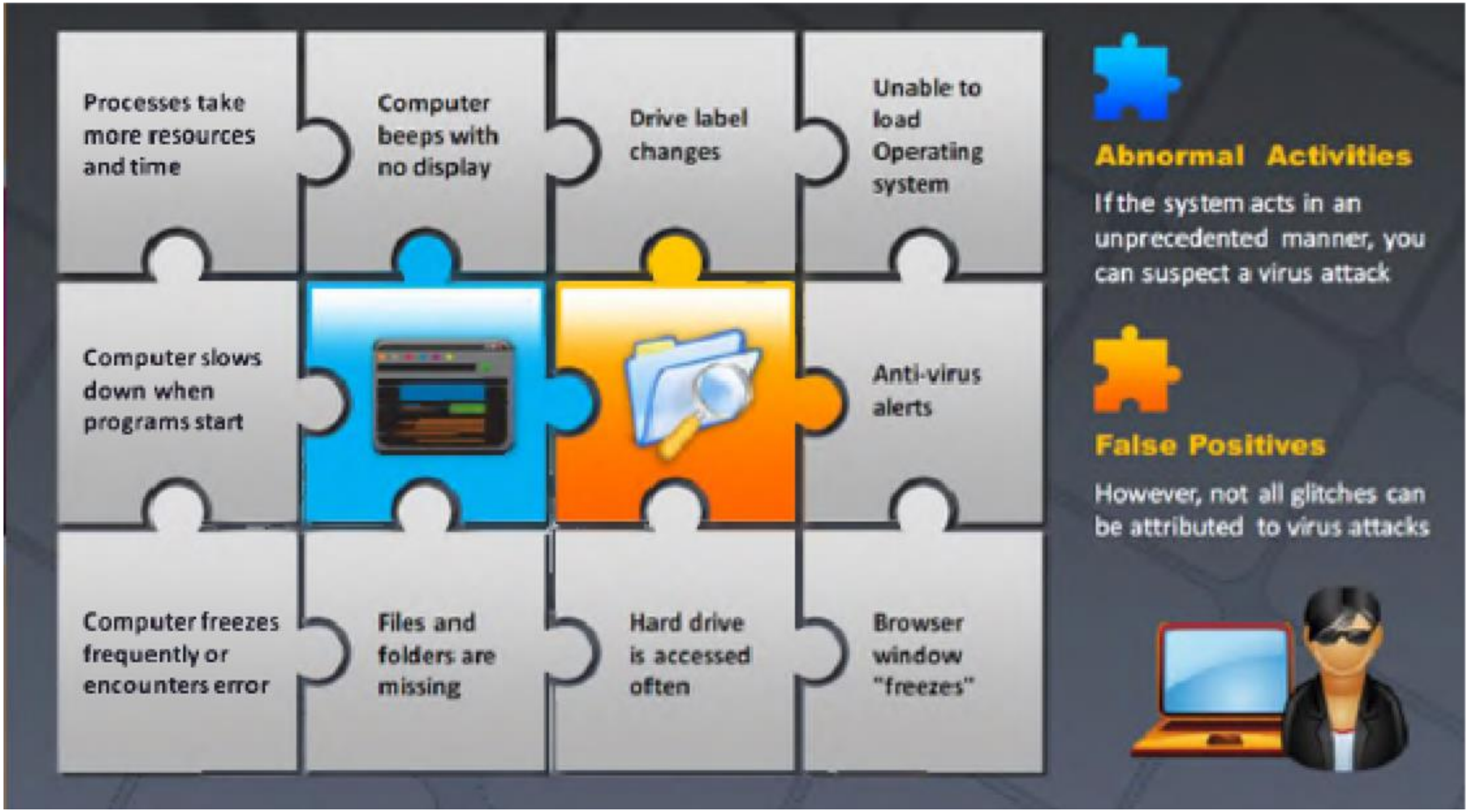
Computer Viruses

- ✓ Inflict damage to competitors
- ✓ Financial benefits
- ✓ Research projects
- ✓ Play prank
- ✓ Vandalism
- ✓ Cyber terrorism
- ✓ Distribute political messages

Attacker

Vulnerable System

How to know if virus attacked?



Processes take more resources and time

Computer beeps with no display

Drive label changes

Unable to load Operating system

Computer slows down when programs start

Anti-virus alerts

Computer freezes frequently or encounters error

Files and folders are missing

Hard drive is accessed often

Browser window "freezes"

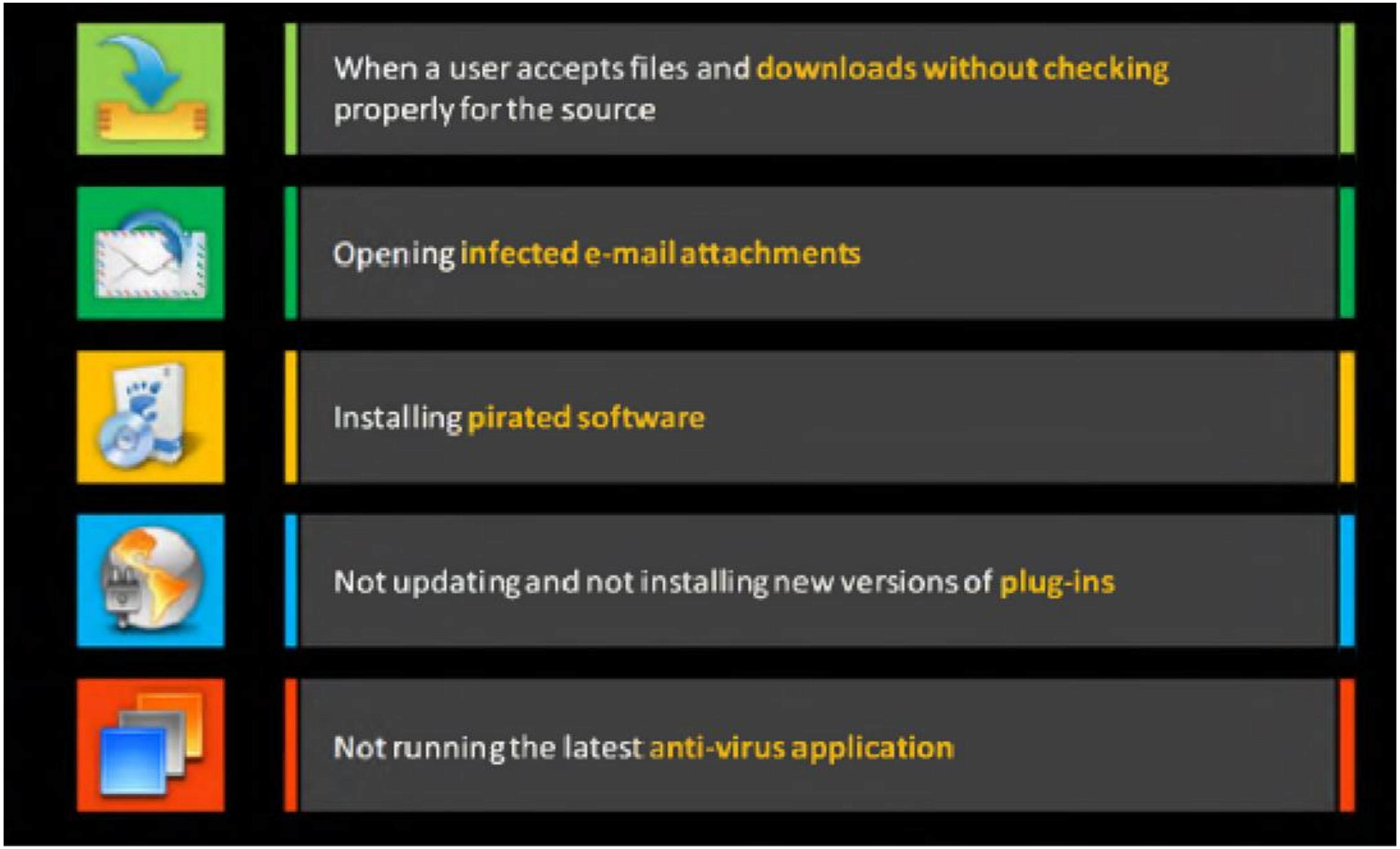
Abnormal Activities

If the system acts in an unprecedented manner, you can suspect a virus attack

False Positives

However, not all glitches can be attributed to virus attacks

Reasons for computer infection



When a user accepts files and downloads without checking properly for the source

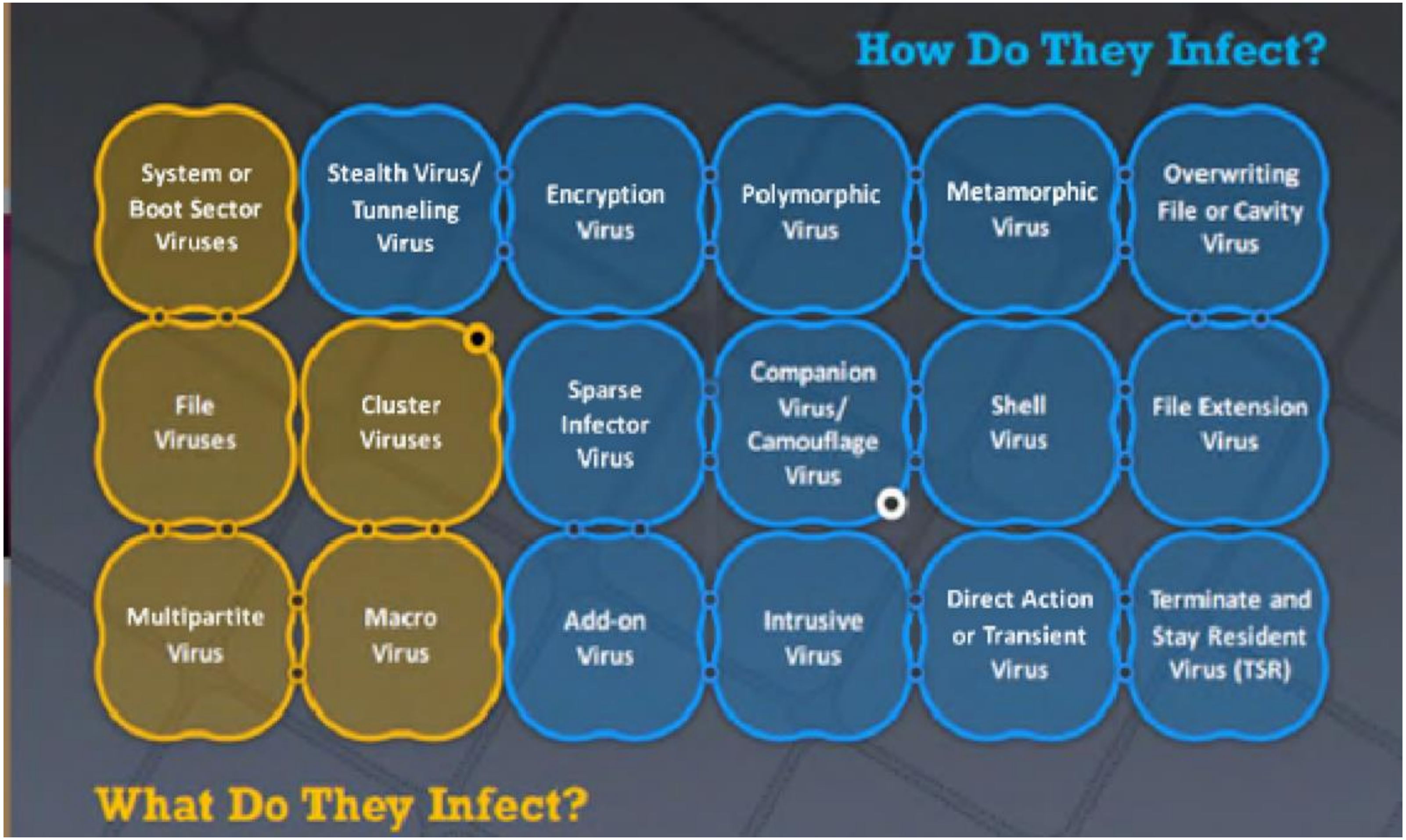
Opening infected e-mail attachments

Installing pirated software

Not updating and not installing new versions of plug-ins

Not running the latest anti-virus application

Virus - infection types



How Do They Infect?

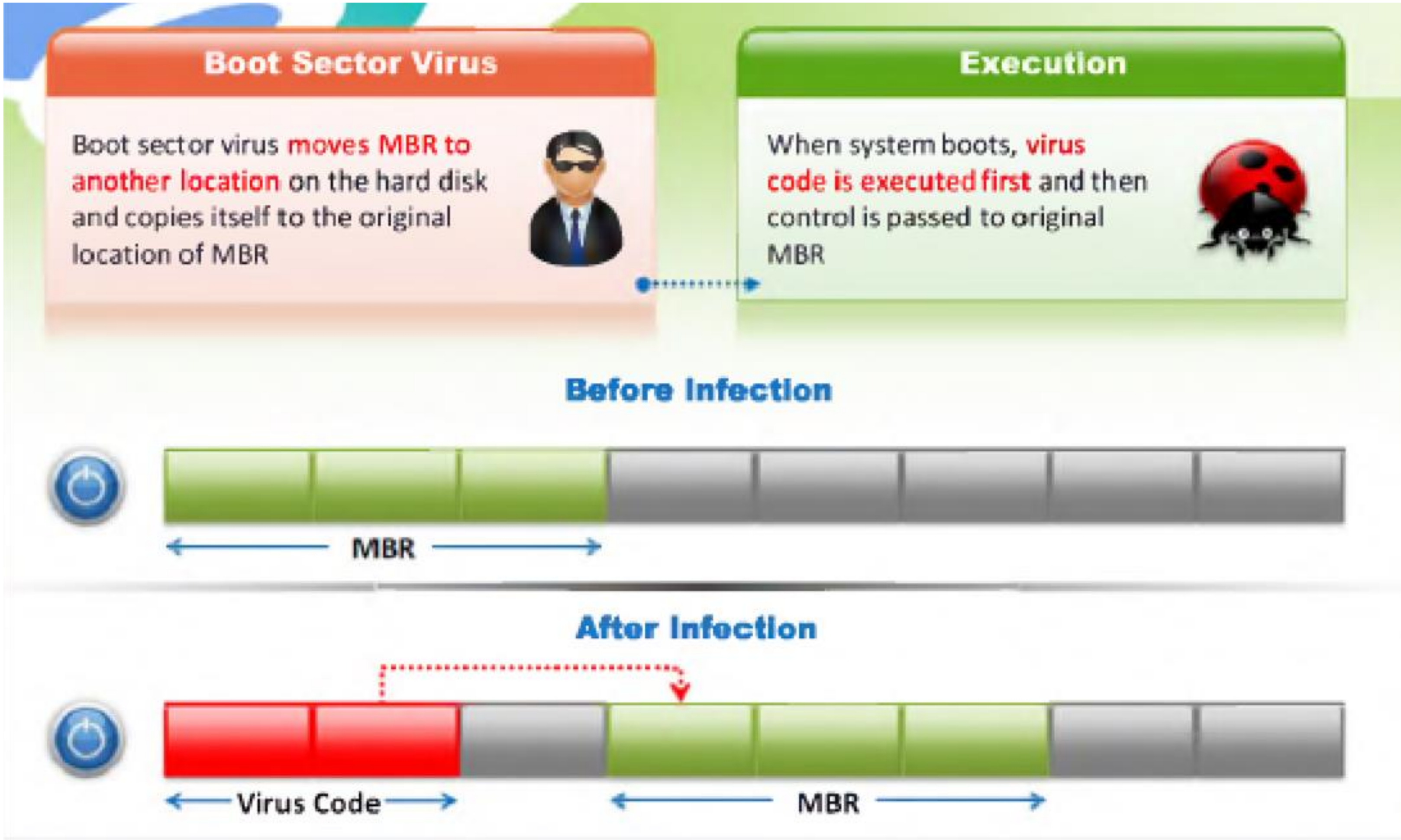
System or Boot Sector Viruses	Stealth Virus/ Tunneling Virus	Encryption Virus	Polymorphic Virus	Metamorphic Virus	Overwriting File or Cavity Virus
File Viruses	Cluster Viruses	Sparse Infector Virus	Companion Virus/ Camouflage Virus	Shell Virus	File Extension Virus
Multipartite Virus	Macro Virus	Add-on Virus	Intrusive Virus	Direct Action or Transient Virus	Terminate and Stay Resident Virus (TSR)

What Do They Infect?

POLYMORPHIC VIRUS VERSUS METAMORPHIC VIRUS

POLYMORPHIC VIRUS	METAMORPHIC VIRUS
A hampful, destructive or intrusive type malware that can change, making it difficult to detect with anti-malware programs	A virus that is rewritten with every iteration so that every succeeding version of the code is different from the proceeding one
Encrypts itself with a variable encryption key so that each copy of the virus appears different	Rewrites its code itself to make it appear different each time
Comparatively less difficult to write	More difficult to write
Derected using the Entry Point Algorithm and the Generic Description Technology	Detected using Geometric detection and by using emulators for tracing

System or Boot sector virus



Boot Sector Virus

Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR

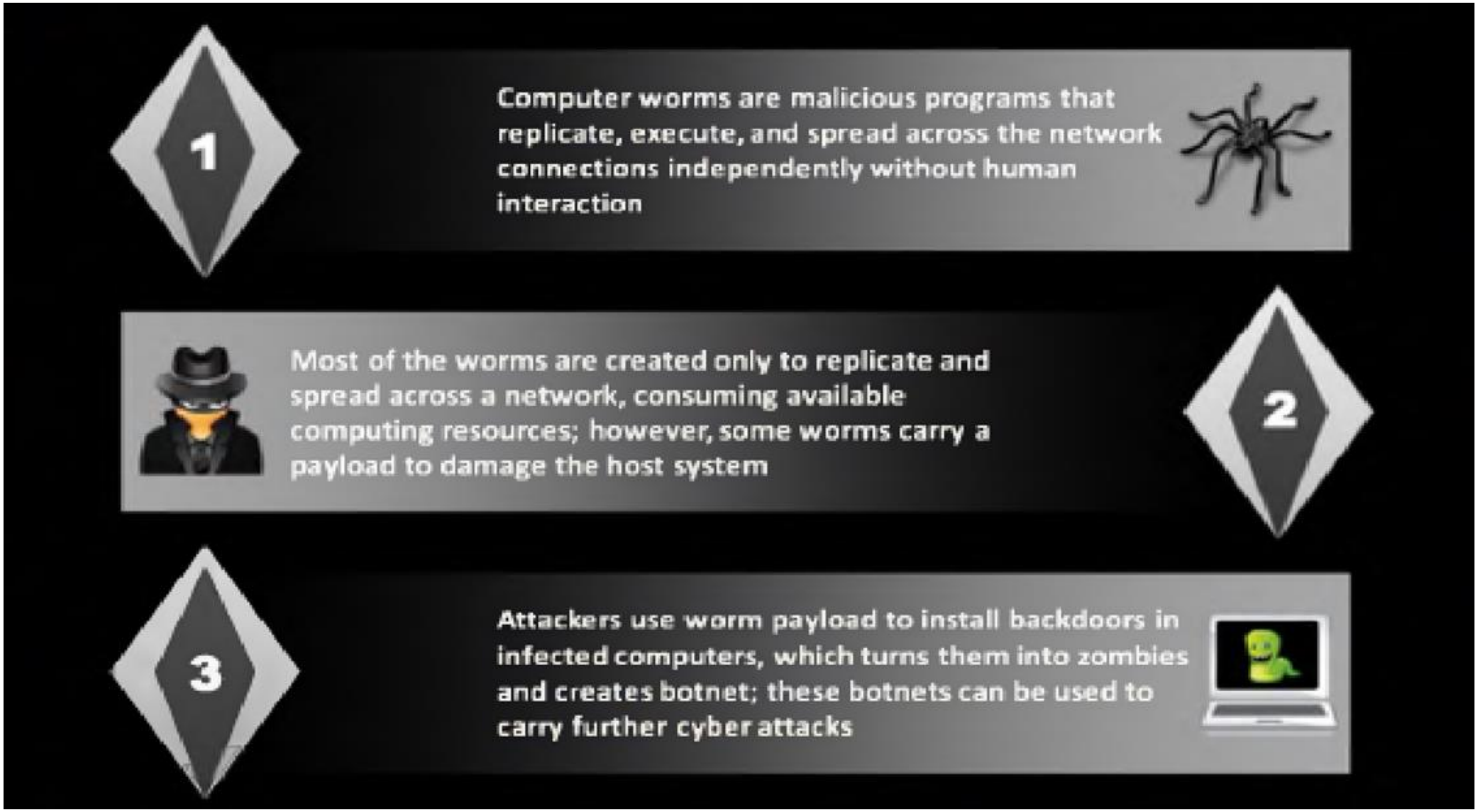
Execution

When system boots, virus code is executed first and then control is passed to original MBR

Before Infection

After Infection

Worms



1

Computer worms are malicious programs that replicate, execute, and spread across the network connections independently without human interaction

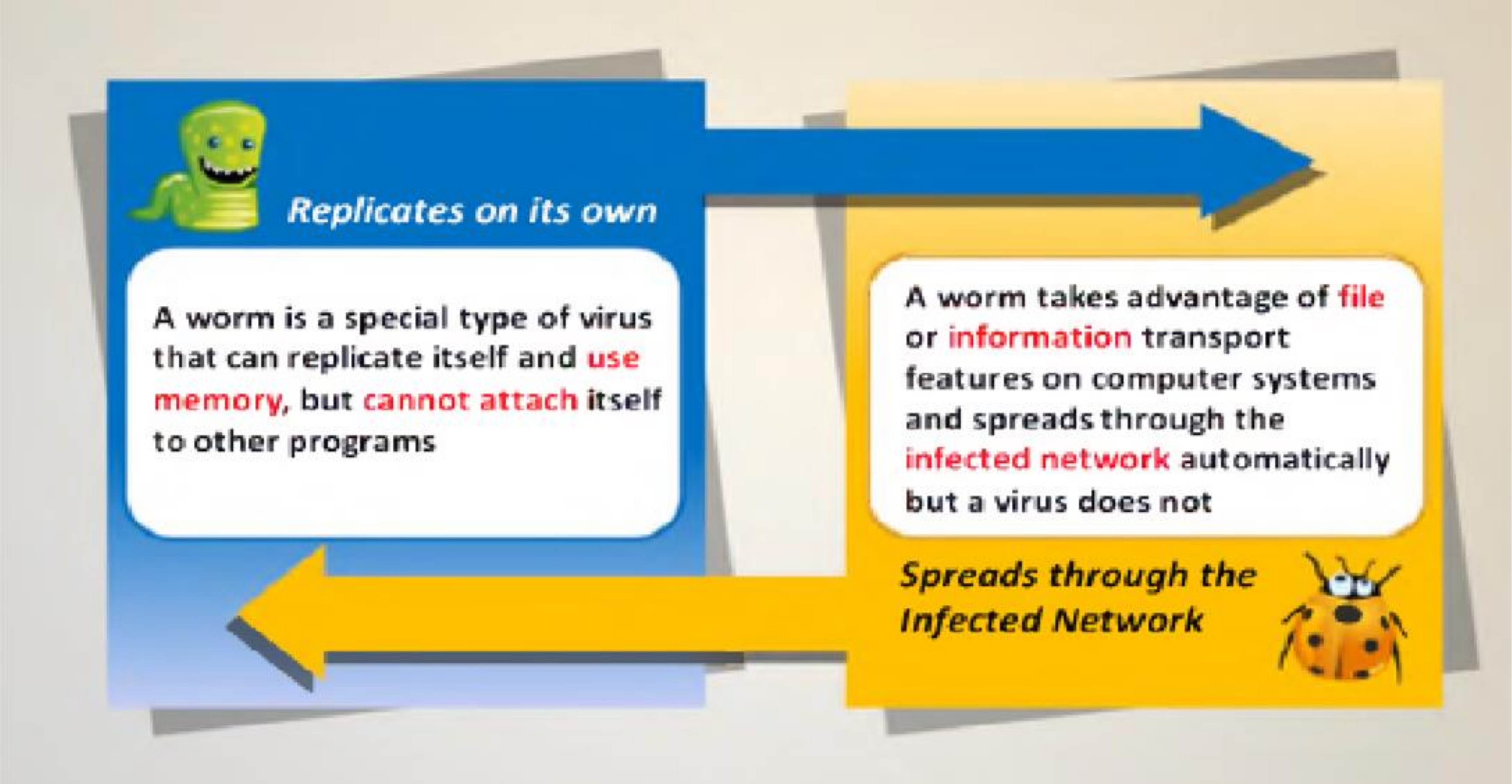
2

Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system

3

Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks

worm Vs virus



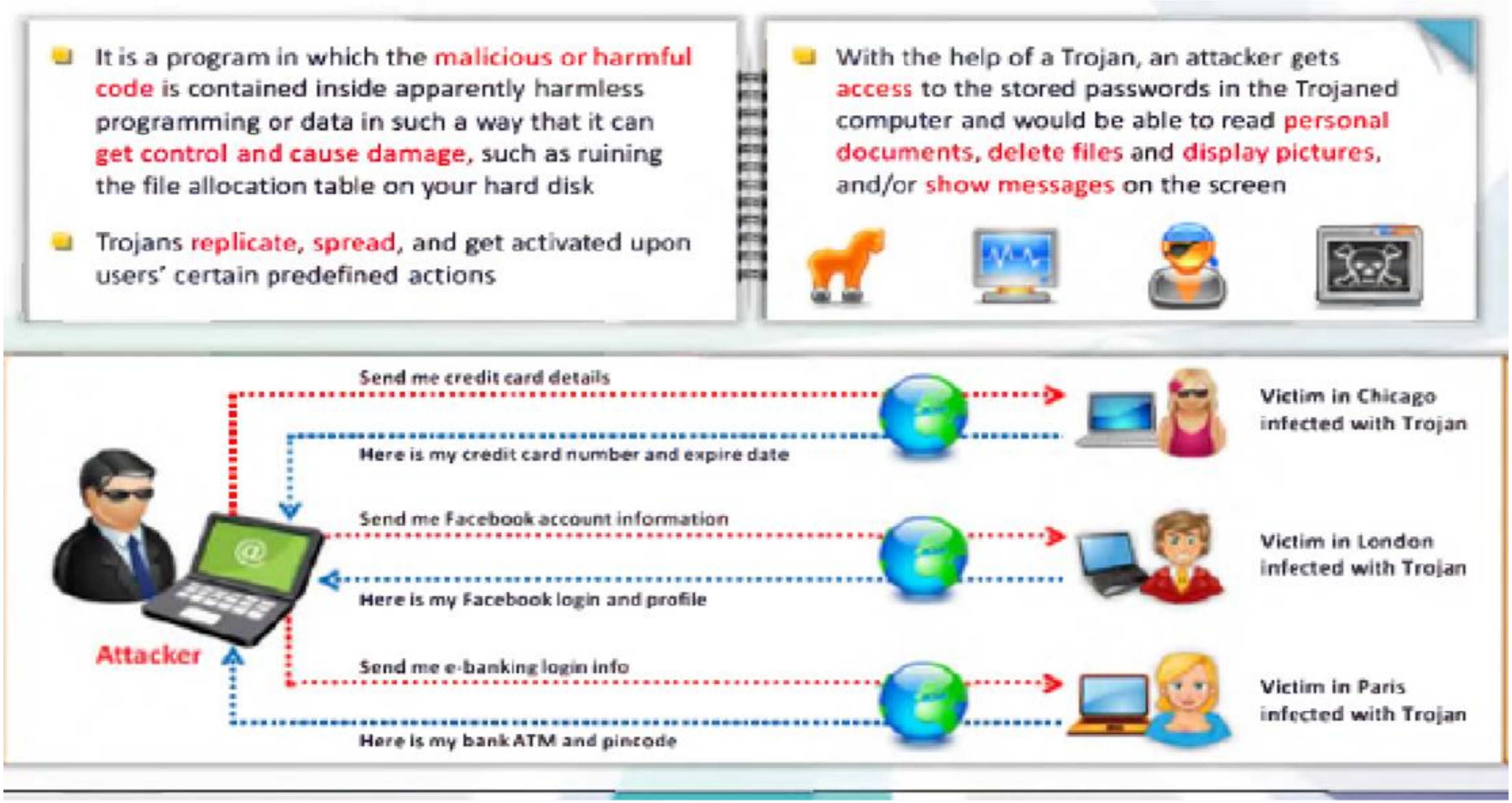
Replicates on its own

A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs

A worm takes advantage of file or information transport features on computer systems and spreads through the infected network automatically but a virus does not

Spreads through the Infected Network

Trojan Horse



- It is a program in which the malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause damage, such as ruining the file allocation table on your hard disk
- Trojans replicate, spread, and get activated upon users' certain predefined actions

- With the help of a Trojan, an attacker gets access to the stored passwords in the Trojaned computer and would be able to read personal documents, delete files and display pictures, and/or show messages on the screen

Send me credit card details

Here is my credit card number and expire date

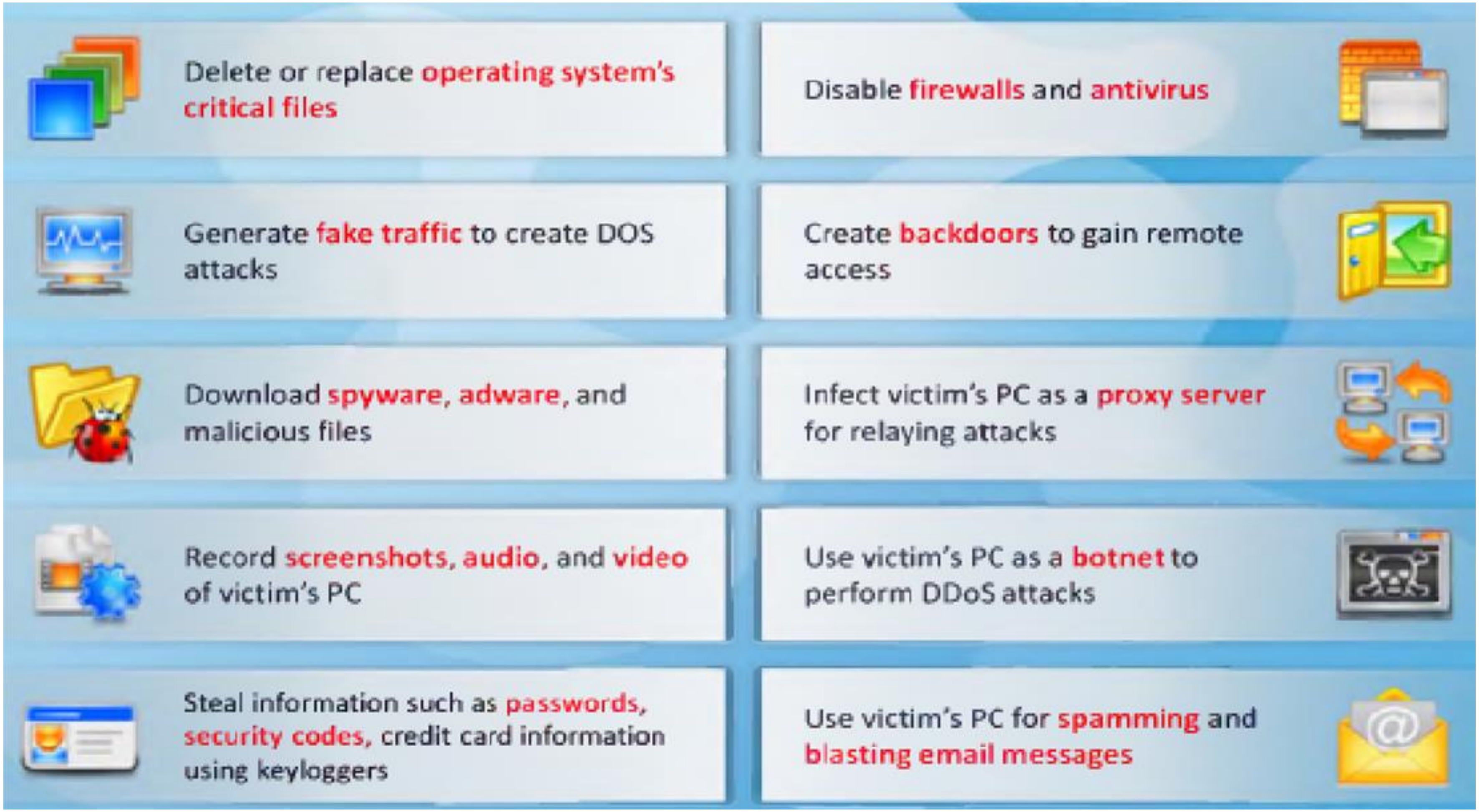
Send me Facebook account information

Here is my Facebook login and profile

Send me e-banking login info

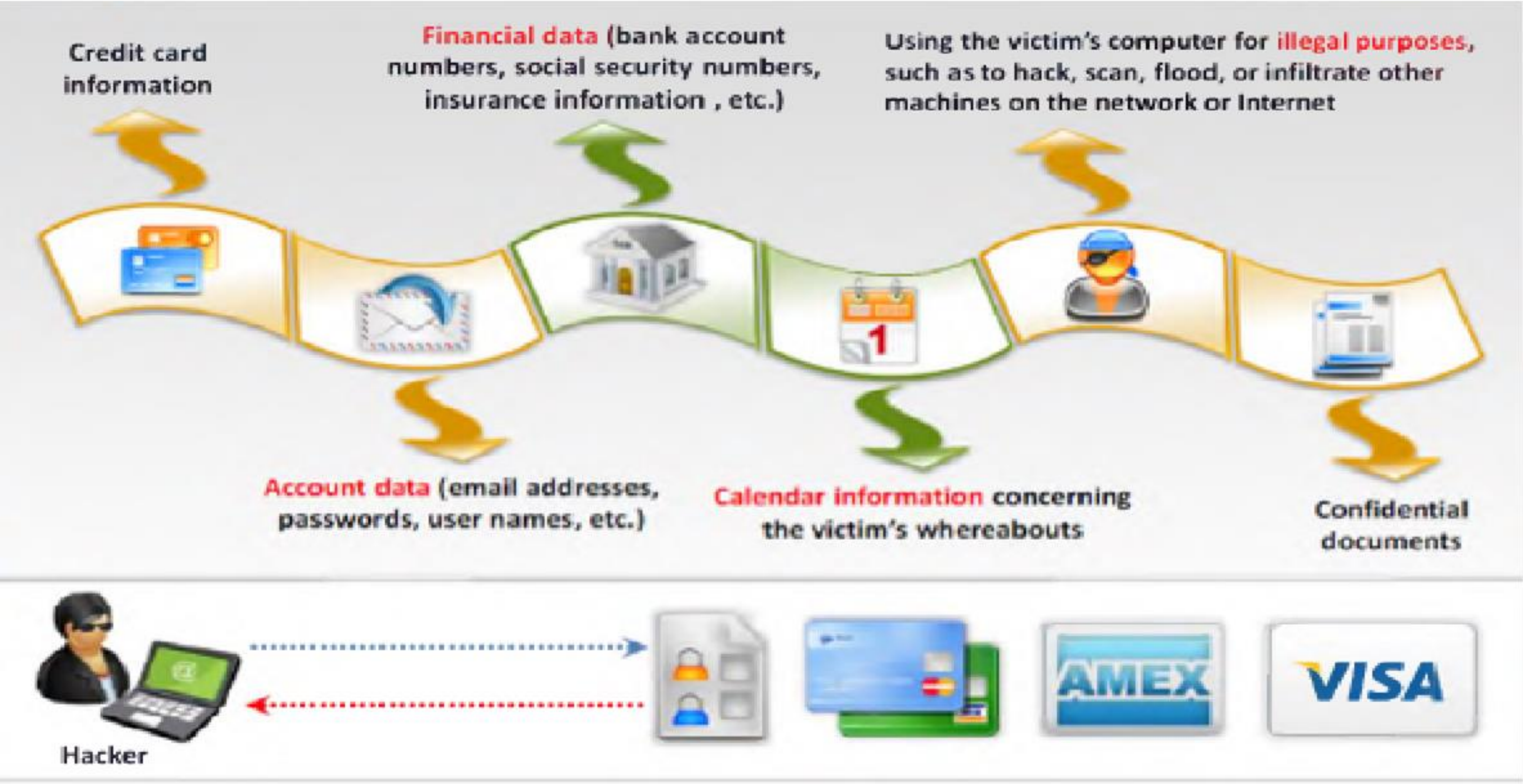
Here is my bank ATM and pincode

Attacker
Victim in Chicago infected with Trojan
Victim in London infected with Trojan
Victim in Paris infected with Trojan



- Delete or replace operating system's critical files
- Generate fake traffic to create DOS attacks
- Download spyware, adware, and malicious files
- Record screenshots, audio, and video of victim's PC
- Steal information such as passwords, security codes, credit card information using keyloggers
- Disable firewalls and antivirus
- Create backdoors to gain remote access
- Infect victim's PC as a proxy server for relaying attacks
- Use victim's PC as a botnet to perform DDoS attacks
- Use victim's PC for spamming and blasting email messages

Reasons for creating trojan horse



Credit card information

Financial data (bank account numbers, social security numbers, insurance information , etc.)

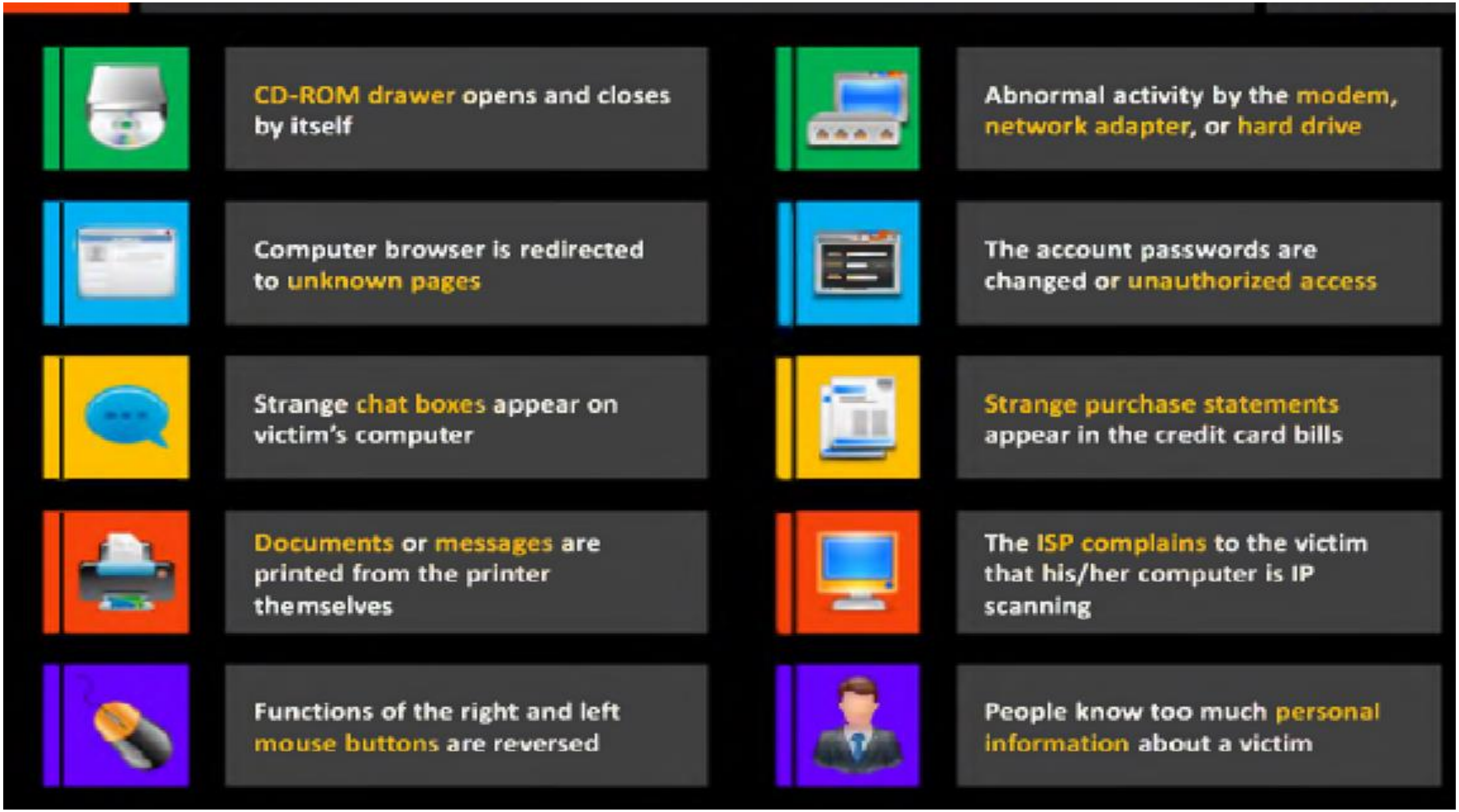
Using the victim's computer for illegal purposes, such as to hack, scan, flood, or infiltrate other machines on the network or Internet

Account data (email addresses, passwords, user names, etc.)

Calendar information concerning the victim's whereabouts

Confidential documents

How to know trojan attack



CD-ROM drawer opens and closes by itself

Abnormal activity by the modem, network adapter, or hard drive

Computer browser is redirected to unknown pages

The account passwords are changed or unauthorized access

Strange chat boxes appear on victim's computer

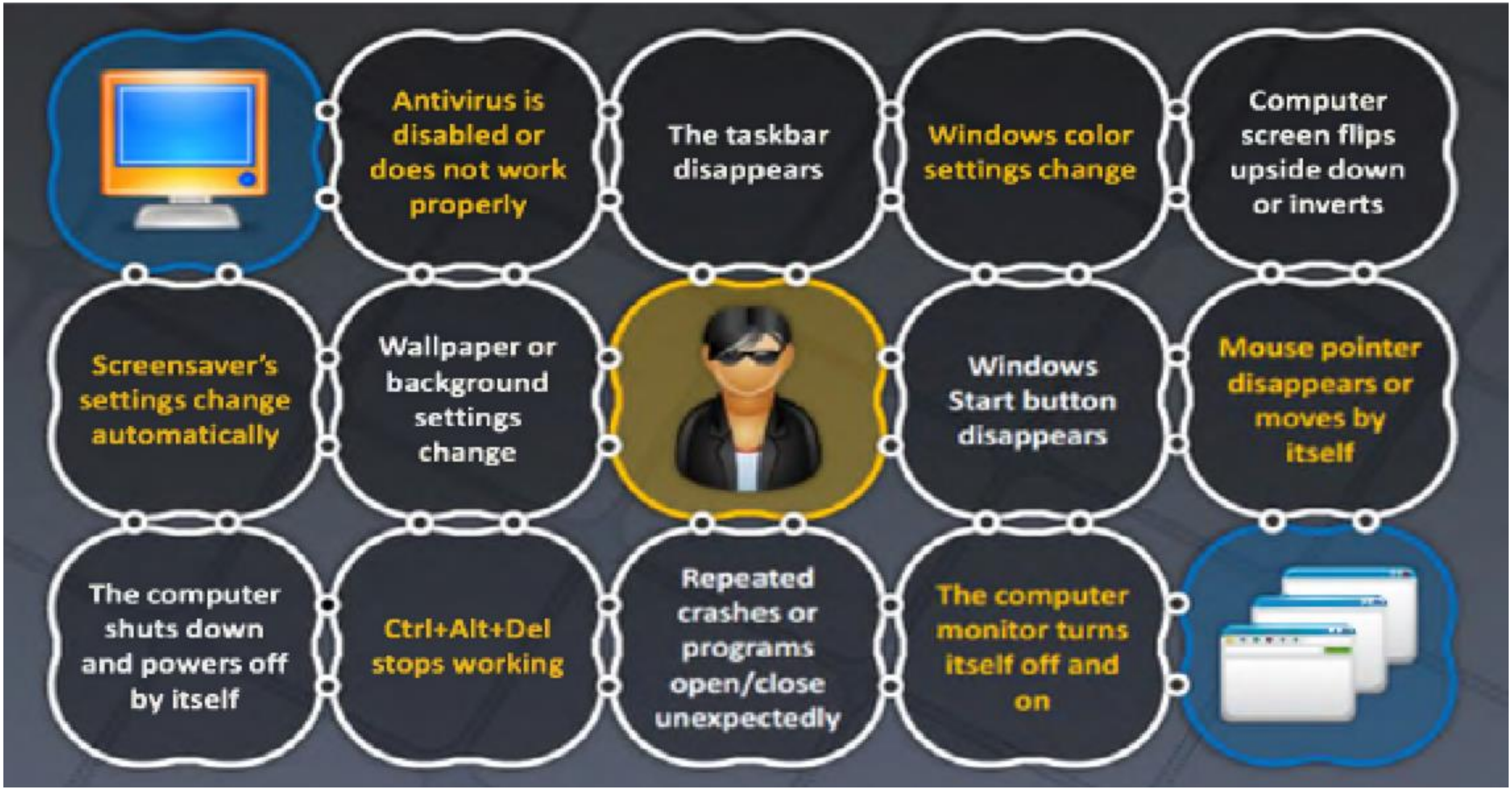
Strange purchase statements appear in the credit card bills

Documents or messages are printed from the printer themselves

The ISP complains to the victim that his/her computer is IP scanning

Functions of the right and left mouse buttons are reversed

People know too much personal information about a victim



Antivirus is disabled or does not work properly

The taskbar disappears

Windows color settings change

Computer screen flips upside down or inverts

Screensaver's settings change automatically

Wallpaper or background settings change

Windows Start button disappears

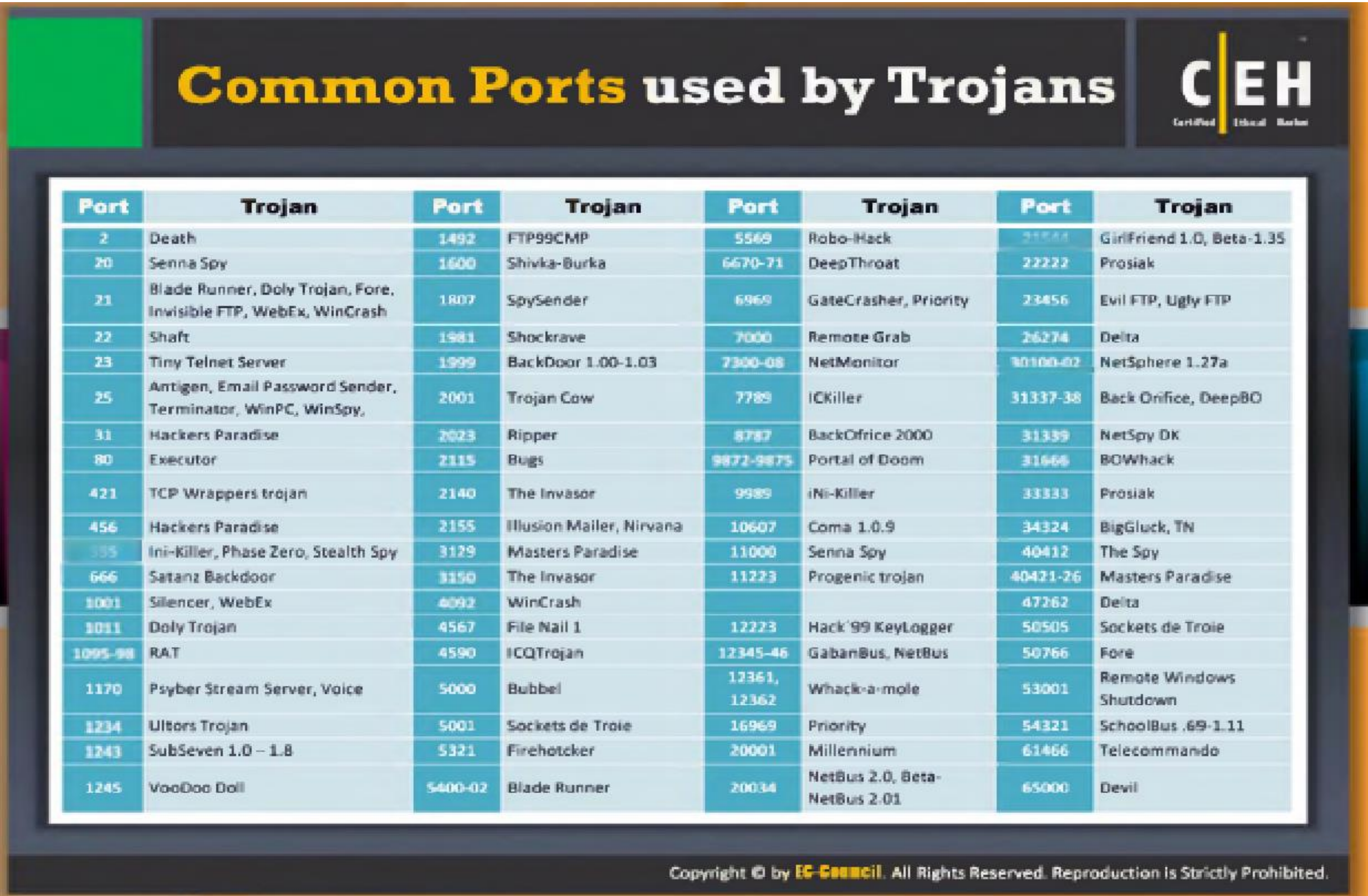
Mouse pointer disappears or moves by itself

The computer shuts down and powers off by itself

Ctrl+Alt+Del stops working

Repeated crashes or programs open/close unexpectedly

The computer monitor turns itself off and on

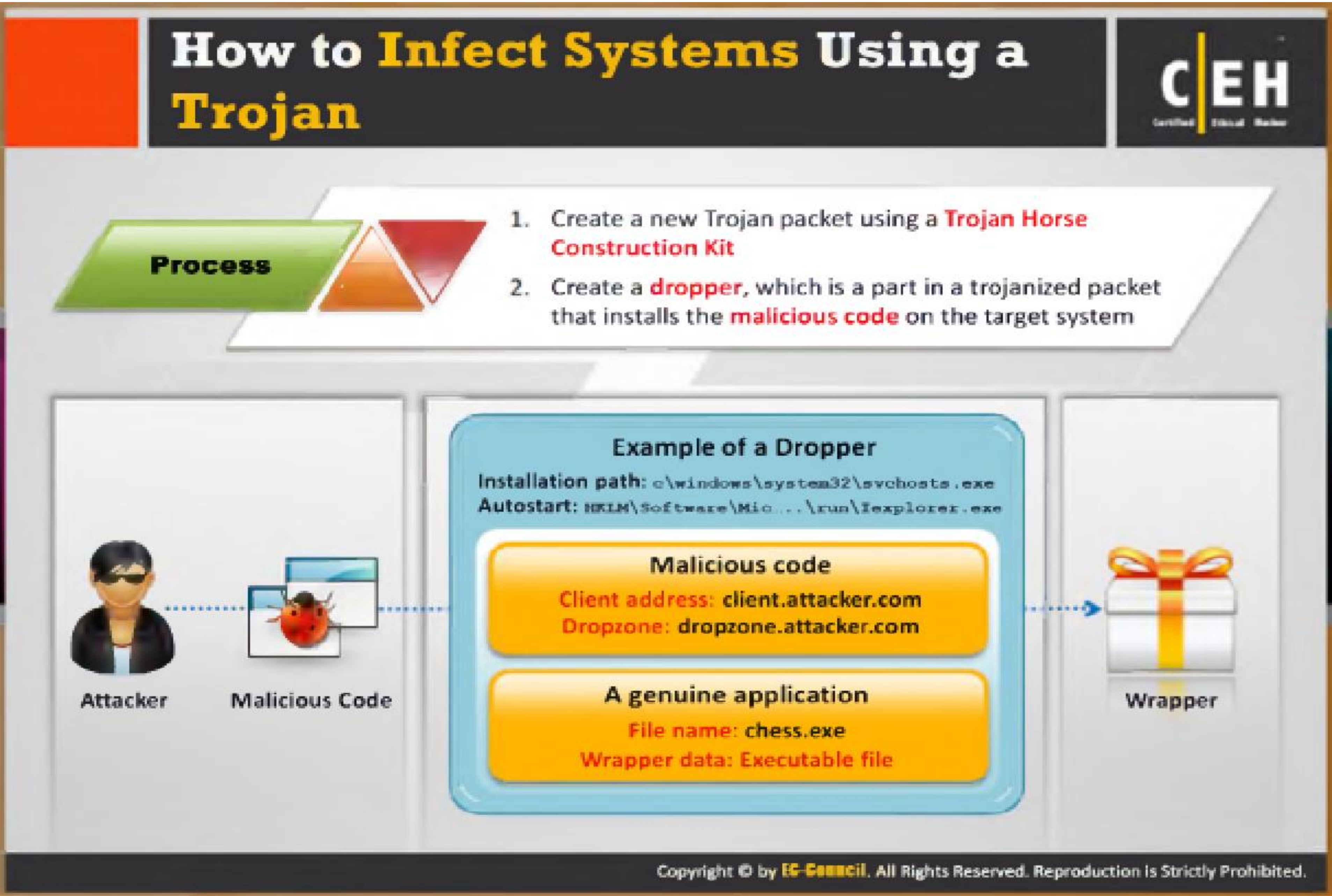


Common Ports used by Trojans

CEH
Certified Ethical Hacker

Port	Trojan	Port	Trojan	Port	Trojan	Port	Trojan
2	Death	1492	FTP99CMP	5569	Robo-Hack	21544	Girlfriend 1.0, Beta-1.35
20	Senna Spy	1600	Shivka-Burka	6670-71	DeepThroat	22222	Prosiak
21	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash	1807	SpySender	6969	GateCrasher, Priority	23456	Evil FTP, Ugly FTP
22	Shaft	1981	Shockrave	7000	Remote Grab	26274	Delta
23	Tiny Telnet Server	1999	BackDoor 1.00-1.03	7300-08	NetMonitor	30100-02	NetSphere 1.27a
25	Antigen, Email Password Sender, Terminator, WinPC, WinSpy,	2001	Trojan Cow	7789	ICKiller	31337-38	Back Orifice, DeepBO
31	Hackers Paradise	2023	Ripper	8787	BackOfrice 2000	31339	NetSpy DK
80	Executor	2115	Bugs	9872-9875	Portal of Doom	31666	BOWhack
421	TCP Wrappers trojan	2140	The Invasor	9989	iNi-Killer	33333	Prosiak
456	Hackers Paradise	2155	Illusion Mailer, Nirvana	10607	Coma 1.0.9	34324	BigGluck, TN
555	Ini-Killer, Phase Zero, Stealth Spy	3129	Masters Paradise	11000	Senna Spy	40412	The Spy
666	Satanz Backdoor	3150	The Invasor	11223	Progenic trojan	40421-26	Masters Paradise
1001	Silencer, WebEx	4092	WinCrash			47262	Delta
1011	Doly Trojan	4567	File Nail 1	12223	Hack´99 KeyLogger	50505	Sockets de Troie
1095-98	RAT	4590	ICQTrojan	12345-46	GabanBus, NetBus	50766	Fore
1170	Psyber Stream Server, Voice	5000	Bubbel	12361, 12362	Whack-a-mole	53001	Remote Windows Shutdown
1234	Ultors Trojan	5001	Sockets de Troie	16969	Priority	54321	SchoolBus .69-1.11
1243	SubSeven 1.0 – 1.8	5321	Firehotcker	20001	Millennium	61466	Telecommando
1245	VooDoo Doll	5400-02	Blade Runner	20034	NetBus 2.0, Beta-NetBus 2.01	65000	Devil

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



How to Infect Systems Using a Trojan

Process

1. Create a new Trojan packet using a **Trojan Horse Construction Kit**
2. Create a **dropper**, which is a part in a trojanized packet that installs the **malicious code** on the target system

Example of a Dropper

Installation path: `c\windows\system32\svchosts.exe`

Autostart: `HKLM\Software\Mic...\run\Iexplorer.exe`

Malicious code

Client address: client.attacker.com

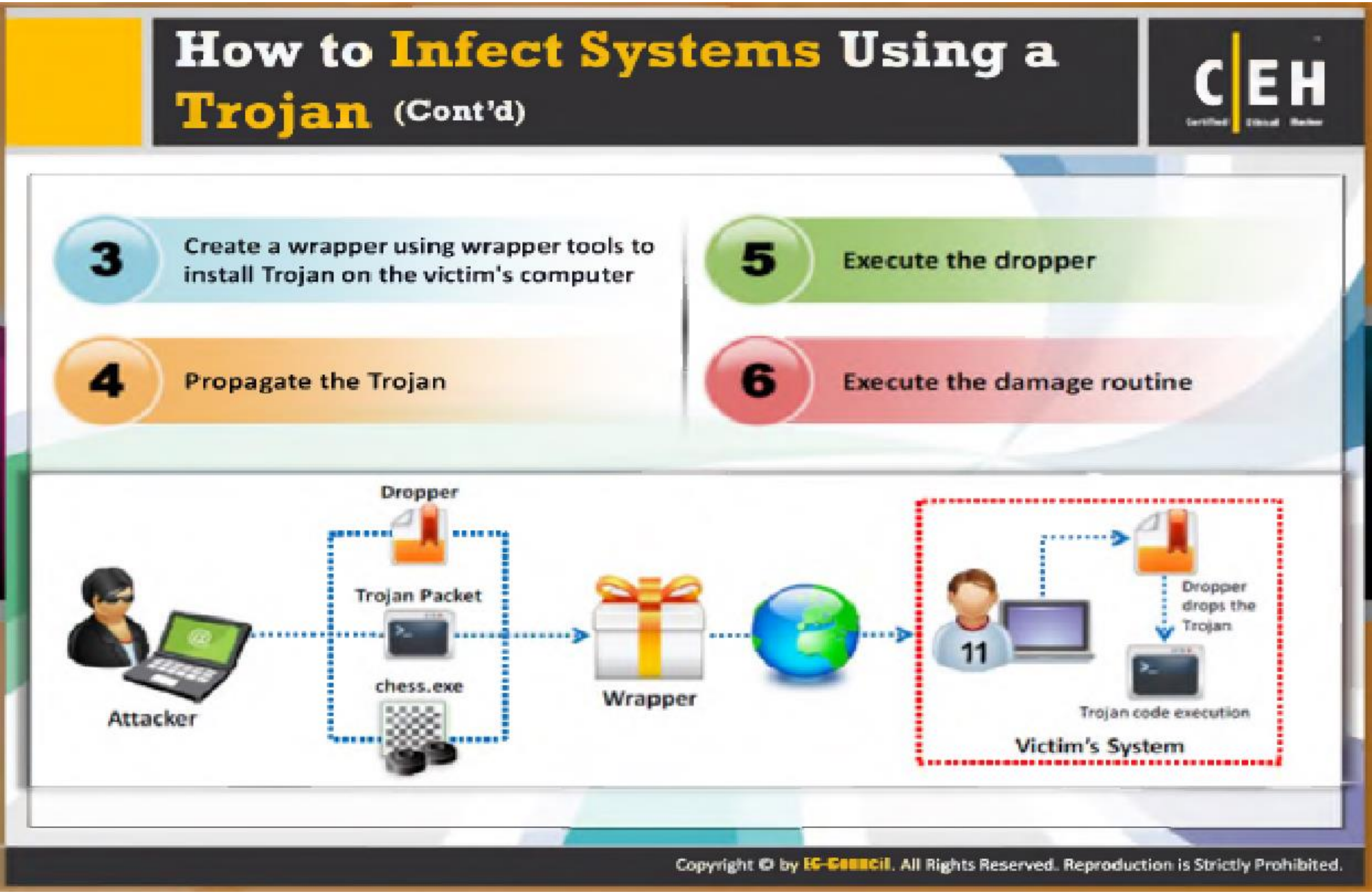
Dropzone: dropzone.attacker.com

A genuine application

File name: chess.exe

Wrapper data: Executable file

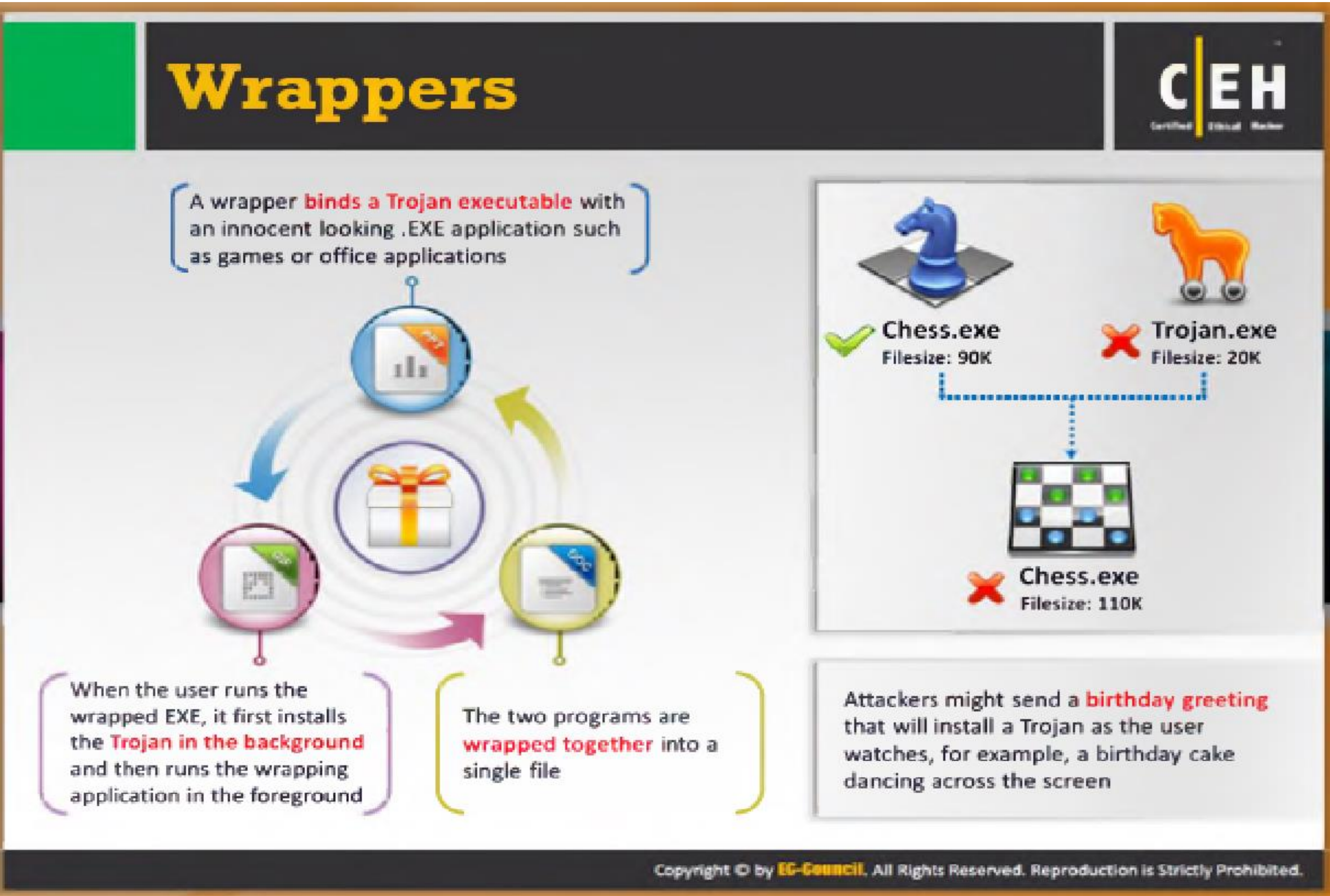
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



How to Infect Systems Using a Trojan (Cont'd)

3. Create a wrapper using wrapper tools to install Trojan on the victim's computer
4. Propagate the Trojan
5. Execute the dropper
6. Execute the damage routine

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Wrappers

A wrapper **binds a Trojan executable** with an innocent looking .EXE application such as games or office applications

When the user runs the wrapped EXE, it first installs the **Trojan in the background** and then runs the wrapping application in the foreground

The two programs are **wrapped together** into a single file

✓ Chess.exe
Filesize: 90K

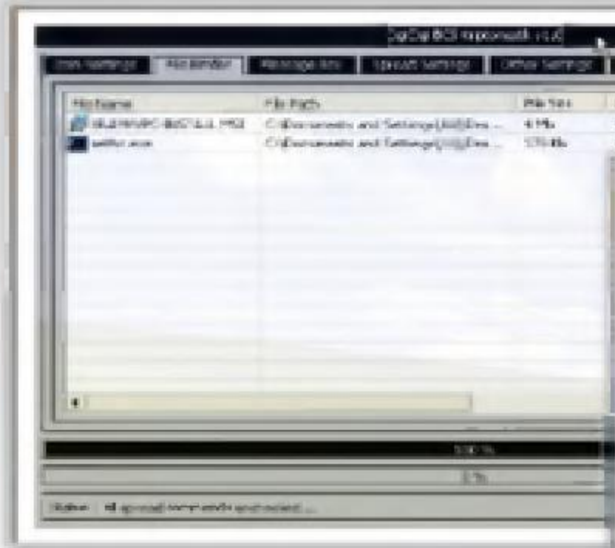
✗ Trojan.exe
Filesize: 20K

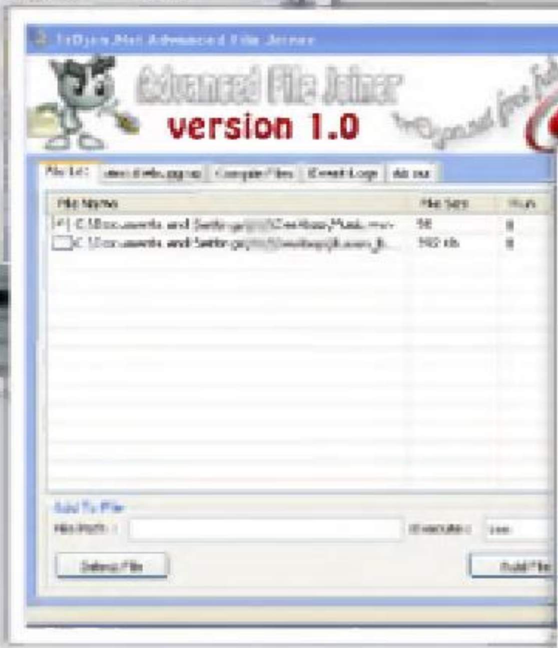
✗ Chess.exe
Filesize: 110K

Attackers might send a **birthday greeting** that will install a Trojan as the user watches, for example, a birthday cake dancing across the screen

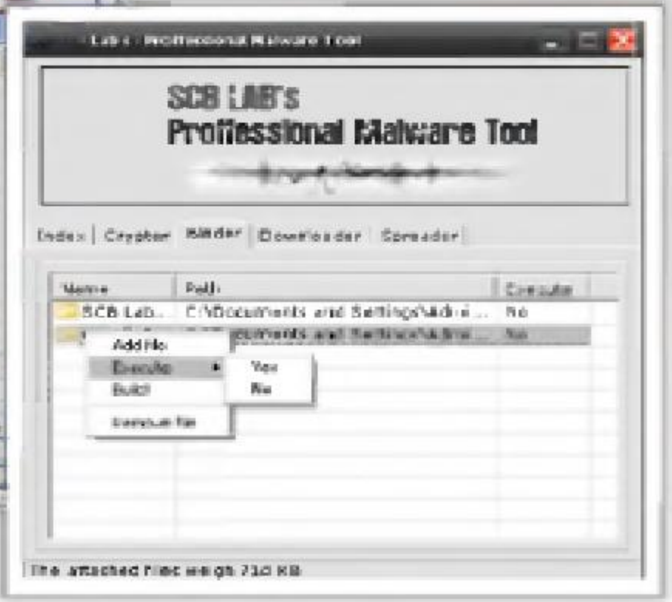
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wrapper Covert Programs


Kriptomatik



Advanced File Joiner

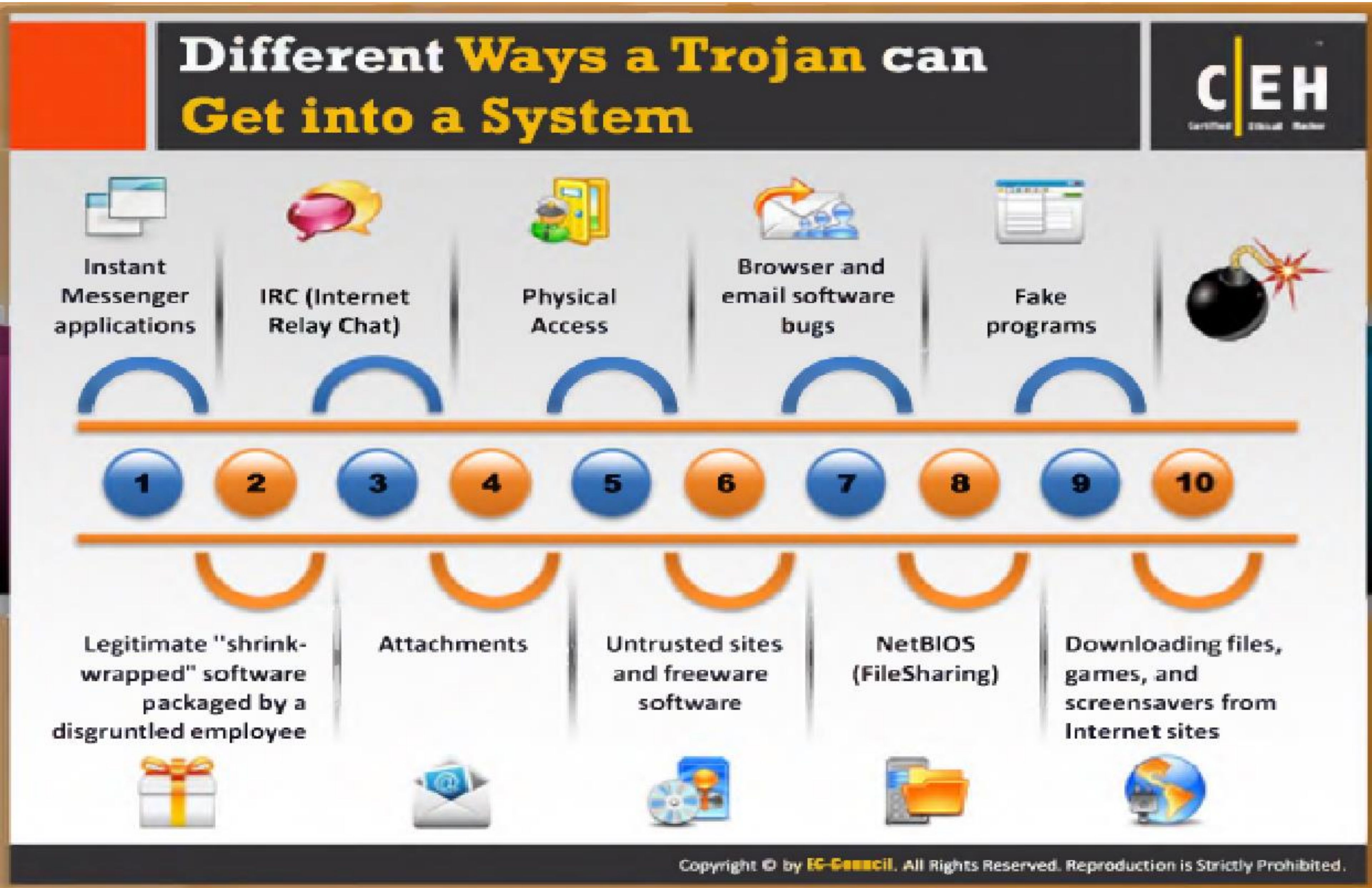


SCB LAB...   C:\Documents and Settings\Admi...   No

The attached files weigh 710 KB

SCB LAB's – Professional Malware Tool

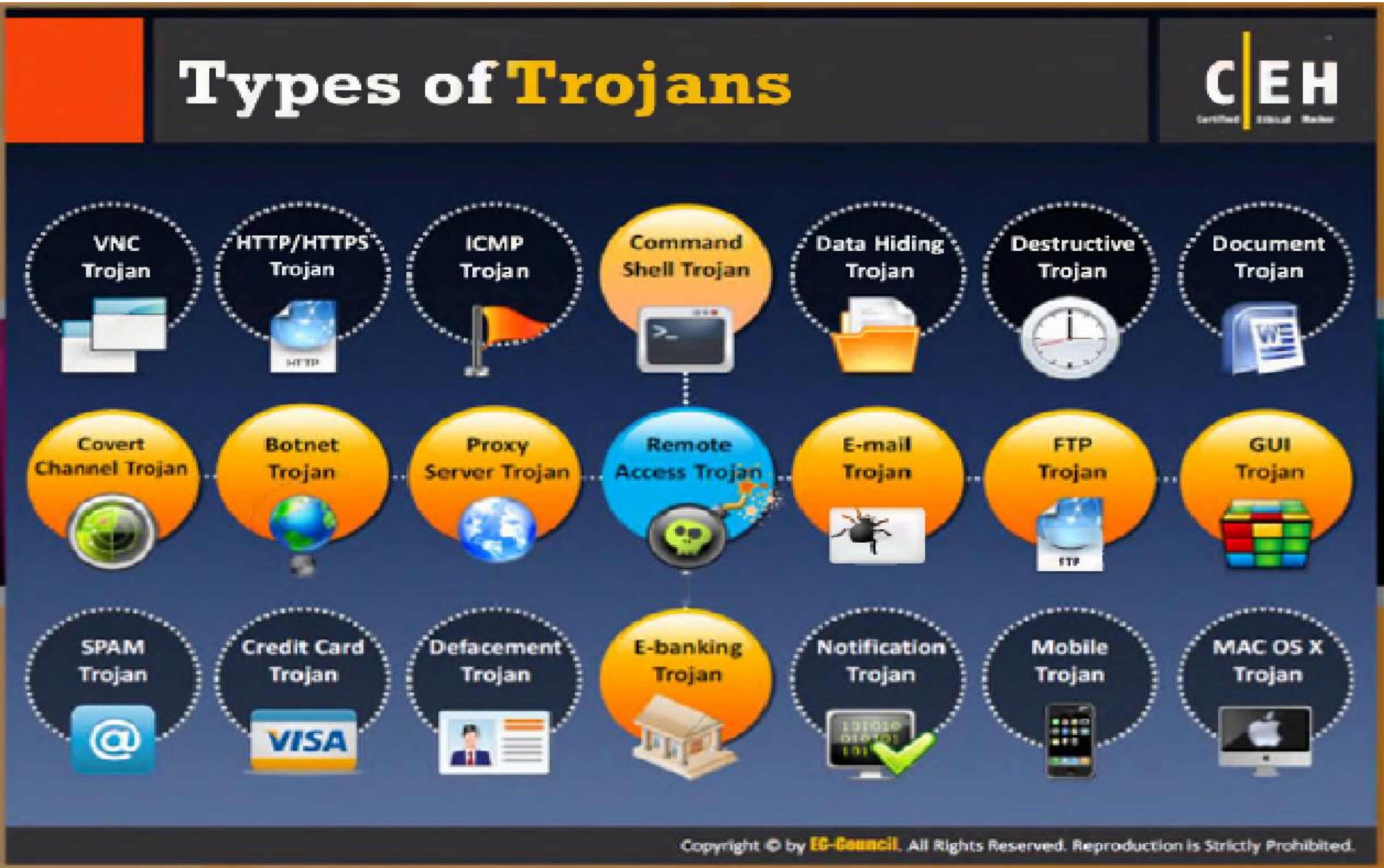
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Different Ways a Trojan can Get into a System

1. Instant Messenger applications
2. Legitimate "shrink-wrapped" software packaged by a disgruntled employee
3. IRC (Internet Relay Chat)
4. Attachments
5. Physical Access
6. Untrusted sites and freeware software
7. Browser and email software bugs
8. NetBIOS (FileSharing)
9. Fake programs
10. Downloading files, games, and screensavers from Internet sites

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

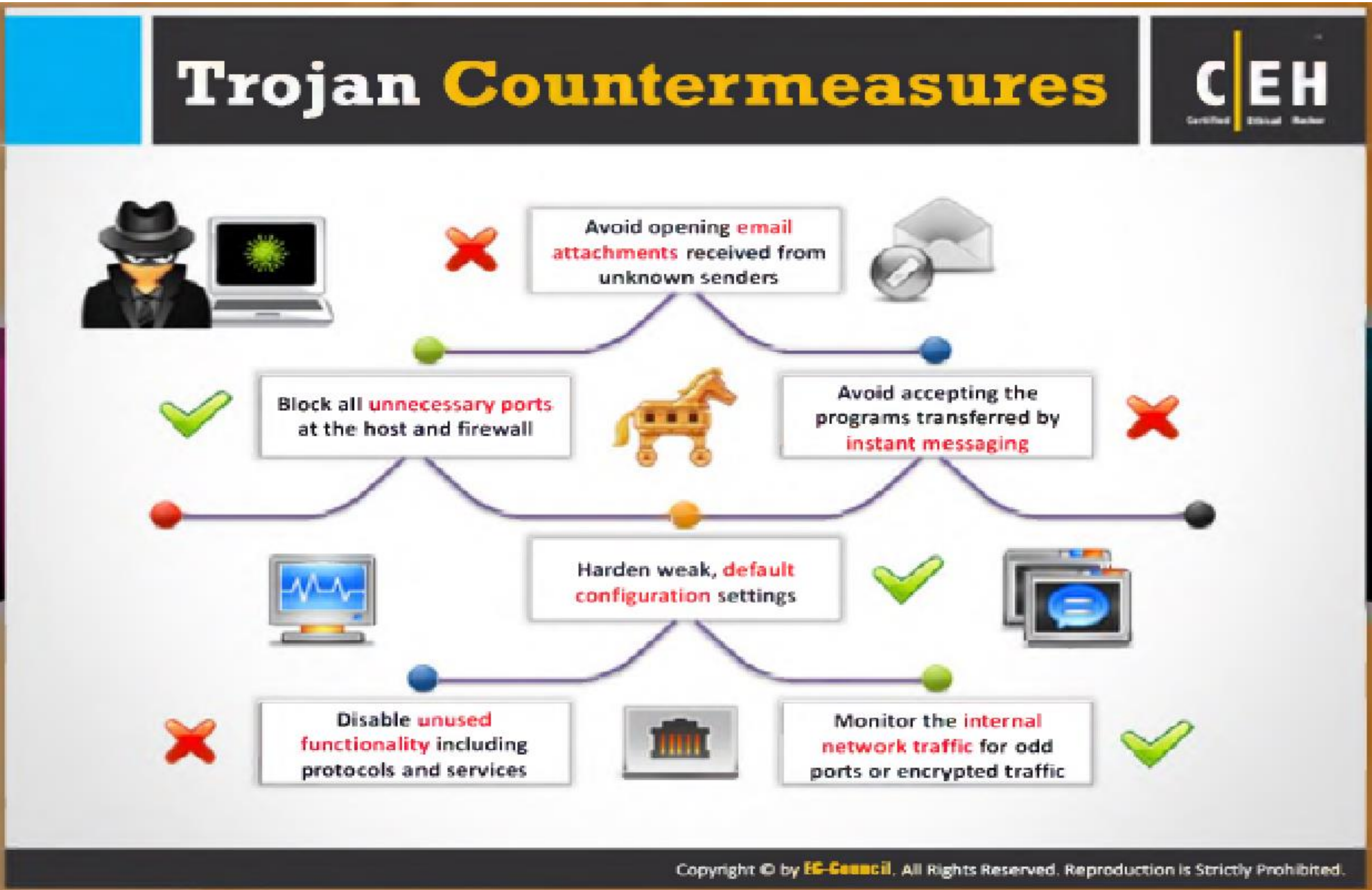


Types of Trojans

C|EH

- VNC Trojan
- HTTP/HTTPS Trojan
- ICMP Trojan
- Command Shell Trojan
- Data Hiding Trojan
- Destructive Trojan
- Document Trojan
- Covert Channel Trojan
- Botnet Trojan
- Proxy Server Trojan
- Remote Access Trojan
- E-mail Trojan
- FTP Trojan
- GUI Trojan
- SPAM Trojan
- Credit Card Trojan
- Defacement Trojan
- E-banking Trojan
- Notification Trojan
- Mobile Trojan
- MAC OS X Trojan

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Trojan Countermeasures

✗ Avoid opening email attachments received from unknown senders

✓ Block all unnecessary ports at the host and firewall

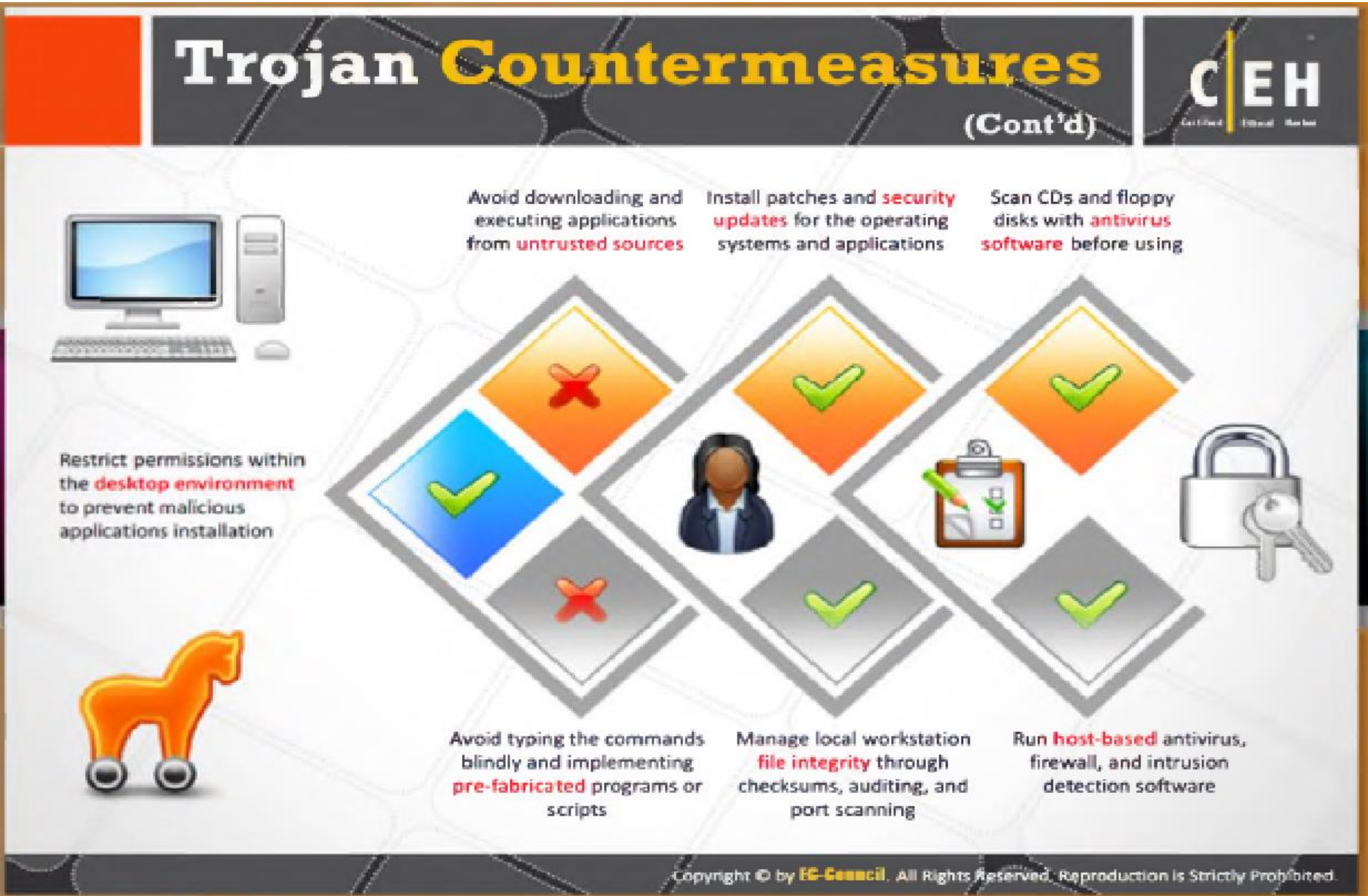
Avoid accepting the programs transferred by instant messaging ✗

Harden weak, default configuration settings ✓

✗ Disable unused functionality including protocols and services

Monitor the internal network traffic for odd ports or encrypted traffic ✓

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Trojan Countermeasures (Cont'd)

Restrict permissions within the **desktop environment** to prevent malicious applications installation

Avoid downloading and executing applications from **untrusted sources**

Install patches and **security updates** for the operating systems and applications

Scan CDs and floppy disks with **antivirus software** before using

Avoid typing the commands blindly and implementing **pre-fabricated** programs or scripts

Manage local workstation **file integrity** through checksums, auditing, and port scanning

Run **host-based** antivirus, firewall, and intrusion detection software

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.