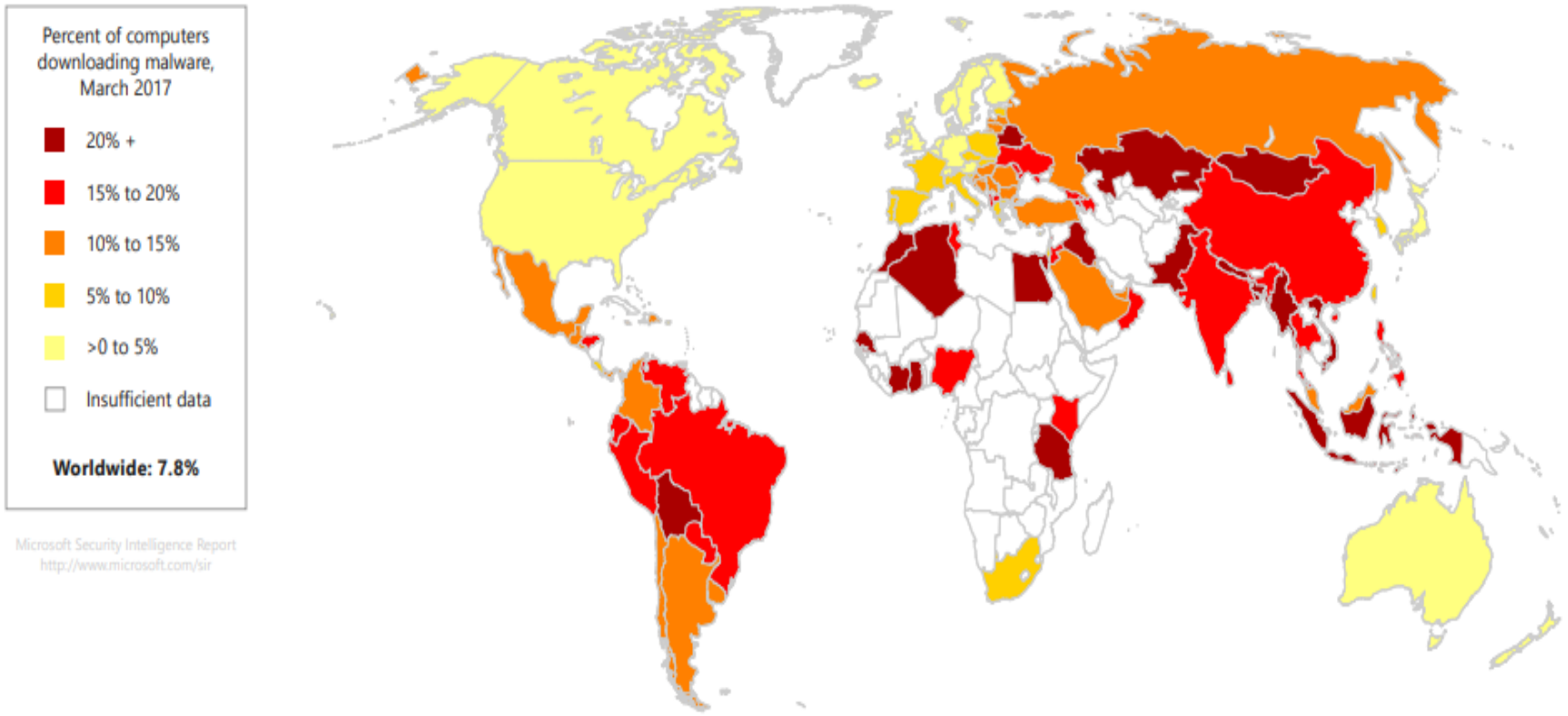
Cyber Threats

Pr. NoureddineChikouche
noureddine.chikouche@univ-msila.dz
https://sites.google.com/view/chikouchenoureddine

Course outline

- Malware
- Email threats
- Protection

Encounter rate by country in March 2017



Source: Trends in GlobalCybersecurity,Microsift, 2017

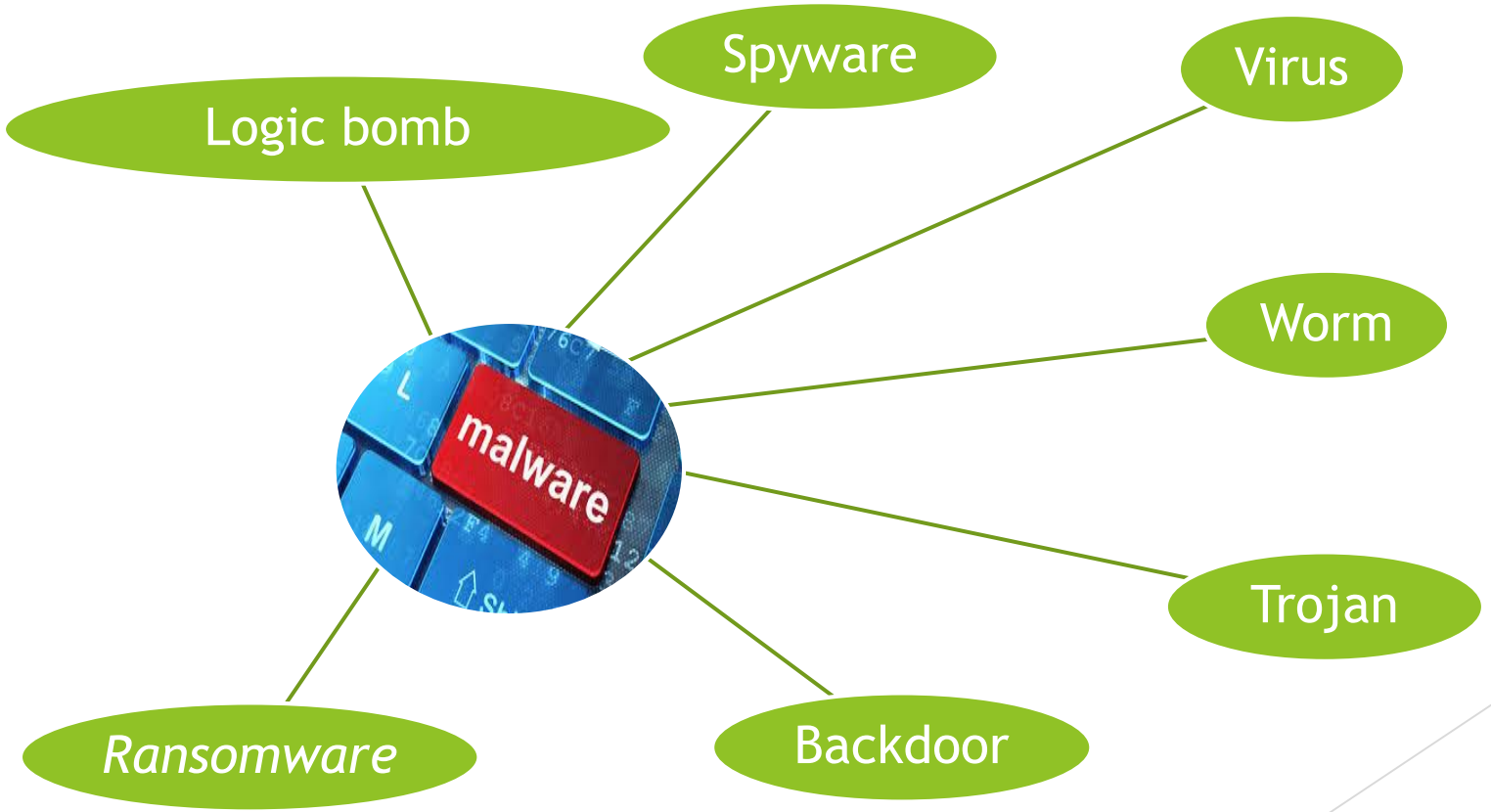
Threat category prevalence, worldwide and in 10 locations with the most computers reporting encounters

Category	Worldwide	Algeria	Bangladesh	Egypt	Indonesia	Iraq	Myanmar	Nepal	Pakistan	Palestinian Authority	Vietnam
Trojans	6.2	19.5	22.3	20.2	17.4	17.0	18.9	16.4	21.6	17.4	18.6
Worms	1.1	8.9	6.8	5.6	8.0	6.7	6.7	7.9	14.1	6.7	3.1
Downloaders & Droppers	0.7	2.1	1.7	2.3	1.2	1.1	1.1	2.0	2.2	1.1	0.7
Viruses	0.7	1.5	3.1	2.6	3.7	2.2	3.7	2.1	2.8	2.3	2.4
Other Malware	0.4	1.1	0.9	1.1	1.0	0.8	0.8	0.8	1.3	1.2	0.9
Obfuscators & Injectors	0.2	1.2	0.9	0.9	0.6	0.7	0.5	0.5	0.7	0.8	0.4
Backdoors	0.2	1.0	0.5	0.7	0.3	2.3	0.8	0.3	0.8	1.1	0.4
Password Stealers & Monitoring Tools	0.1	0.2	0.2	0.2	0.2	0.1	0.3	0.2	0.2	0.2	0.2
Ransomware	0.1	0.2	0.2	0.3	0.2	0.1	0.1	0.2	0.2	0.2	0.1
Exploits	0.1	0.2	0.1	0.2	0.2	0.1	0.2	0.1	0.1	0.2	0.1

Source: Trends in Global Cybersecurity,Microsift, 2017

Malware

Malware is software developed with the intention of harming a computer system.



Malware

Virus:

- A virus is a program that runs on a device and can spread to other devices within an information system in order to disrupt computer applications.
- Resident viruses load into the computer's RAM to infect executable files launched by the user.
- Non-resident viruses infect programs on the hard drive as soon as they are executed.

Virus

They can contaminate machines in several ways:

- Downloading and running software without taking precautions.
- data exchange (Flash disk, Bluetooth, …).
- Opening documents with macros without taking precautions
- Email attachments (.exe.vbs).
- Opening an HTML email containing JavaScript that exploits a software security vulnerability.
- Exploiting a bug in the email software.

Prevention: Virus

- Be wary of an attached file name or an email subject that is too attractive.
- Never open an attachment with an extension (.exe, .com, .bat, .vbs, .pif,).
- Be wary of Word (.doc), Excel (.xls) or PowerPoint (.pps) containing macros in Visual Basic;
- Never open a file containing a double extension, such as "TrucMuche.GIF.VBS", which are tricks used to hide the true identity of an infected file.

Prevention: Virus

- Never trust the sender, even if it's someone you know. Some worms use the address books of infected computers to spread.
- Do not insert discs without knowing their origin.
- Back up your important files regularly, because even with the utmost vigilance.
- Install antivirus software and regularly update virus definitions.
- Check the origin of files downloaded from the Internet (verify with your antivirus software that they are not infected).
- Delete all unsolicited emails (e.g., spam).

Worm

- It is a type of virus that spreads through the network.
- exploits a computer's network communications to ensure its reproduction on other computers
- In 1988, the student Robber T. Morris developed a worm that infected several thousand computers within 8 hours of being launched.

Worm

- They can spread to outdated machines through email applications and in the form of code executed directly by the email client (JavaScript, VBS, etc.).
- Worms have a promising future in web applications, as social networks (Facebook, X) have seen the emergence of scripts using the languages of these applications or JavaScript, which can spread to the accounts of all users of these services.

Example ?

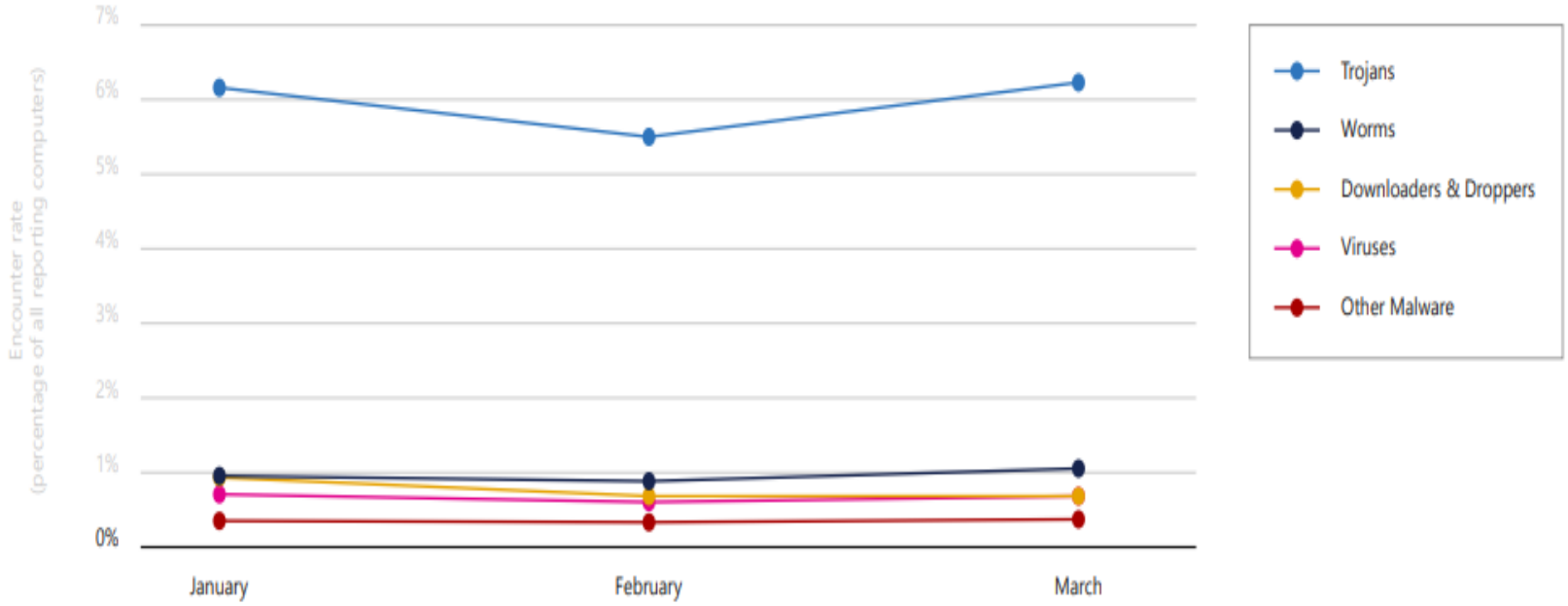
Stuxnet

- Specific to the Windows system, it was discovered in June 2010 by VirusBlokAda.
- It targets systems using Siemens SCADA WinCC/PCS 7 software.
- The first worm discovered that spies on and reprograms industrial systems.
- The worm has affected 45,000 computer systems, including 30,000 located in Iran, including PCs belonging to employees of the Bushehr nuclear power plant.

Trojan horse

- A seemingly legitimate (or intentionally so) computer program that executes harmful routines and hidden, malicious actions without the user's permission.
- It opens a backdoor into a system to allow hackers or other unwanted programs to enter.

Encounter rates for significant malicious software categories in 1Q17



Source: Trends in GlobalCybersecurity,Microsift, 2017

Trojan Horse

- A Trojan horse can, for example:
  - stealing passwords
  - to carry out any other harmful action, etc.
  - copying sensitive data
- Detecting such a program is difficult because it is necessary to be able to detect whether the operation of the program (the Trojan horse) is desired or not by the user.

Trojan Horse

- **Examples:** TrojanZulu, Happy 99,Backdoor,BackOrifice
- Trojan.ByteVerify
  - Trojan horse in the form of a Java applet.
  - Exploits a weakness in Microsoft's Java virtual machine allowing a hacker to execute arbitrary code on the infected machine.
  - For example, it can change the Internet Explorer homepage.

Trojan Horse

Symptoms of an infection

- Abnormal modem or network card activity: data is being loaded even though there is no user activity.
- curious reactions from the mouse
- impromptu program openings
- repeated crashes.

- **Protection:** An application firewall allows you to stop unauthorized applications from accessing the web. Example:ZoneAlarm.

Spyware

- The spyware is an unwanted program that typically installs itself on a machine. Its function is to retrieve information about a person or company transparently from the user.
- He collects personal information on a user's computer without their permission. This information is then transmitted to a third-party computer.

Spyware

- The information collected may include:
  - websites visited (URLs),
  - keywords used in search engines,
  - analysis of purchases made via the Internet, and even bank payment information (credit card/VISA number),
  - personal information (social security number, etc.).

Spyware

There are three types of spyware:

- Commercial: Profiling of internet users
- Displaying banner ads.
- Spyware: Collecting personal data

Spyware

Tempting Cedar

International Business Times

UK World Business Fintech Technology Science Sport Entertainment Opinion Video Pictures

Smartphones | Cybersecurity | Innovation | Social Media | Games | Motoring

Technology | CyberSecurity

What is Tempting Cedar? Hackers using fake Facebook profiles to spread Android spyware

Security experts believe that the hackers behind the Tempting Cedar spyware may be Lebanese.

By India Ashok

February 23, 2018 05:07 GMT

The spyware steals victims' photos, contacts, call logs and can also spy on conversations when the infected device is within range. The Tempting Cedar spyware can also harvest a victim's geolocation via the infected device to track their location, as well as record surrounding sounds.

Example

Zero-day Attack

NSO GROUP

Update (Sept 1, 2016): Today Apple released security updates for Desktop Safari and Mac OS X. These updates patch the Trident vulnerabilities that identified in this report for desktop users. The Trident vulnerabilities used by NSO could have been weaponized against users of non iOS devices, including OSX.**We encourage all Apple users to install the update as soon as possible**. Citizen Lab is not releasing samples of the attack at this time to protect the integrity of still-ongoing investigations.

This report describes how a government targeted an internationally recognized human rights defender, Ahmed Mansoor, with the Trident, a chain of zero-day exploits designed to infect his iPhone with sophisticated commercial spyware.

Spyware

Protection:

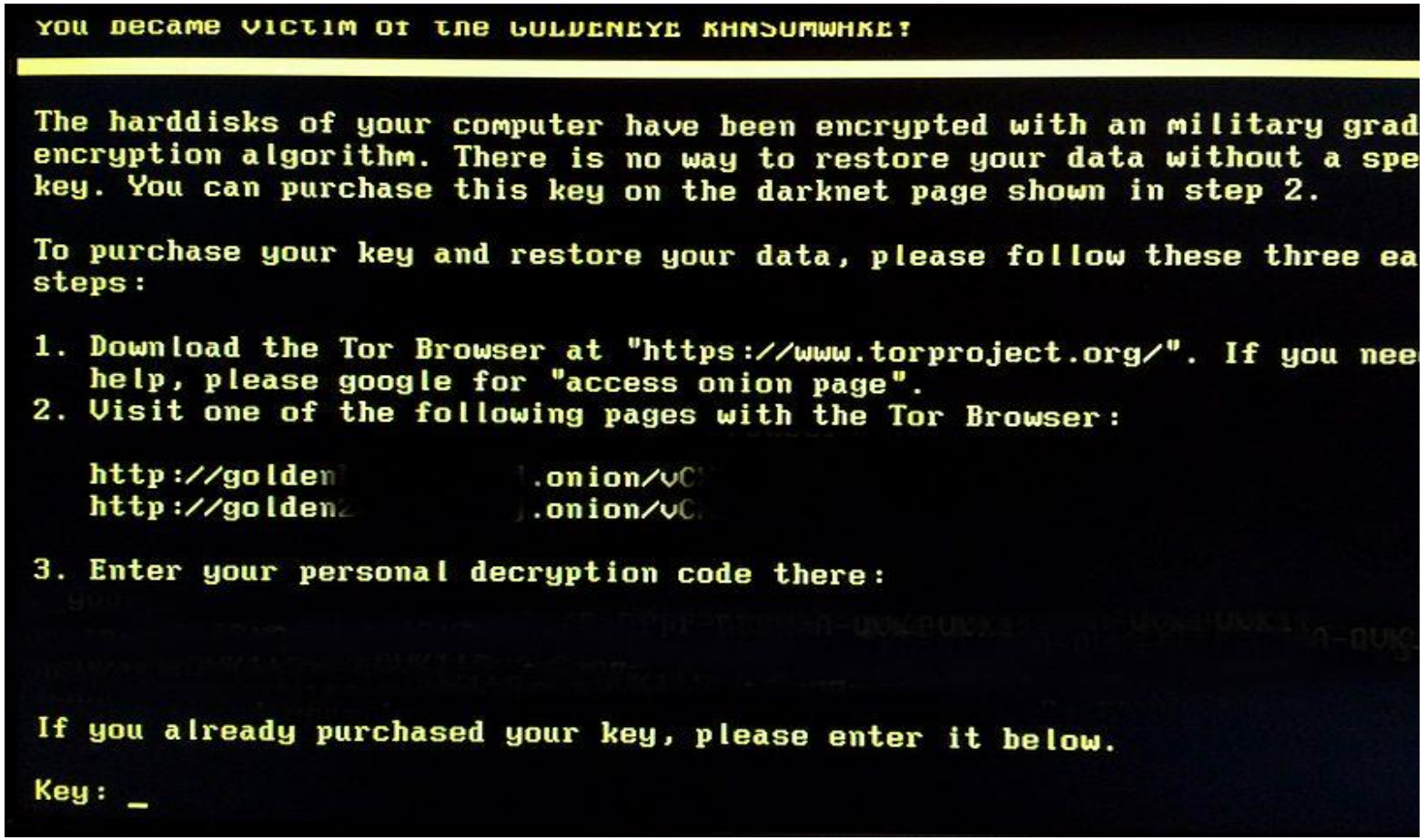
- Installing a personal firewall to detect spyware and prevent it from accessing the internet.
- Using anti-spyware software to detect and remove files, processes, and registry entries created by spyware. Example: Ad-Aware.

Ransomware

- It is malicious software that infects the computer and displays messages demanding payment of a certain sum in order for the system to function again.
- This category can be installed by clicking on misleading links in a e-mail via instant messaging or a website.
- The ransomware has the ability to lock a computer screen (Ransomware Locker) or ofencrypt important files with a password pass (RansomwareCrypto).

SourceKaspersky

Ransomware


You became victim of the GOLDENEYE RANSOMWARE!
The harddisks of your computer have been encrypted with an military grad
encryption algorithm. There is no way to restore your data without a spe
key. You can purchase this key on the darknet page shown in step 2.
To purchase your key and restore your data, please follow these three ea
steps:
1. Download the Tor Browser at "https://www.torproject.org/". If you nee
help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:
http://golden .onion/vC
http://golden .onion/vC
3. Enter your personal decryption code there:
If you already purchased your key, please enter it below.
Key: _

Ransomware

- Examples:
  - Reveton (2012),
  - Ransomware RSA-4096 (april2016),
  - WannaCry (May 2017)
  - Bad Rabbit (october2017)

Backdoor

- hidden communication software, installed for example by a virus or by a Trojan horse,
- It allows for the creation of unauthorized network access to a computer system.
- This makes it possible to remotely exploit the machine.
- Example: it was discovered in the early 2000s in Borland's Interbase DBMS. Simply entering the username "politically" and the password "correct" was enough to connect to the database with administrator privileges.

Keylogger

- A keylogger is a program, usually invisible, installed on a user's computer and designed to record their keystrokes without their knowledge; for example, to intercept passwords.
- Some keyloggers are capable of recording visited URLs, emails read or sent, files opened, and even creating a video recording all computer activity.

Logic bomb

- A logic bomb is a function, hidden within a seemingly honest, useful, or pleasant program, that will trigger after a delay, either when a predetermined time is reached (based on the system's date), or when a specific event occurs.
- This function will then produce unwanted actions.

Logic bomb

- Its primary objective is generally to create a denial-of-service attack by saturating the network connections of an online service, website, or company.
- Examples: Chernobyl, Friday the 13th
- The Chernobyl virus had a logic bomb that activated on April 26, 1999, the thirteenth anniversary of the Chernobyl nuclear disaster.

Course outline

- Main security flaws
- Malware
- Email threats
- Protective Equipment

Unsolicited email (*Spam*)

- The main objective of spam is to advertise cheaply through "mass unsolicited email" or "abusive multi-posting“.
- Spammers collect email addresses from the internet using software (called bots) that crawl various web pages and store all the email addresses found there in a database. Finally, they launch an application that sends the advertising message to each address in turn.

Unsolicited email (*spam*)

Risks:

- The space is occupied by the spam.
- The difficulty of accessing personal or professional messages within numerous spam emails and the increased risk of accidentally deleting or missing important messages;
- The time wasted sorting and deleting unsolicited messages.
- The bandwidth it wastes on the internet.

Protection: anti-spam

Phishing

- Is an email whose sender usually pretends to be a financial institution and asks the recipient to provide confidential information;

Main security flaws

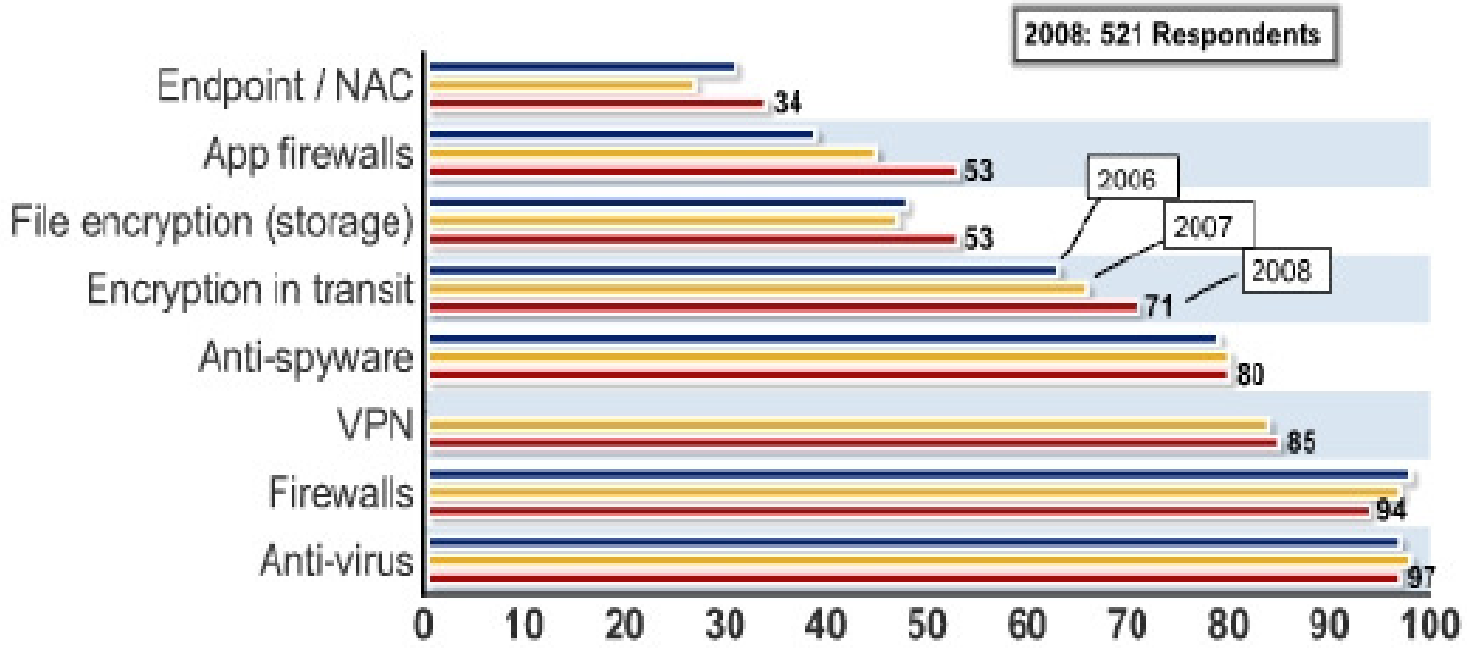
- Installation of default software and hardware
- No operating system updates or patches.
- Non-existent or default passwords
- Complex, unprotected networks
- No separation of operational/system administration flows
- Outdated security procedures
- Weak authentication
- Unnecessary services retained
- Lack of or poor data backup strategy.
- Unsecured access to the computer rooms

Course outline

- Main security flaws
- Malware
- Email threats
- Protection

Some solutions

Figure 16: Security Technologies Used



❶Antivirus

- Antivirus programs are capable of detecting the presence of viruses on a computer, and of cleaning it as much as possible if one or more viruses are found.

❶Antivirus

Antivirus software can be installed primarily in two types of places:

- The entry point to a local network, where traffic from the internet arrives; some of this traffic will be filtered to detect viruses, primarily traffic related to the HTTP (Web) and SMTP (email) protocols.
- The user's workstation, where the antivirus software will generally be used to inspect and disinfect the hard drive (some viruses execute in RAM without being saved to the disk).

❶Antivirus

Antivirus software operates in two ways:

- Static mode: the software is activated only when instructed by the user, for example, to trigger a flash drive inspection.
- Dynamic mode: the software is always active and monitors certain events that occur within the system.
  - It results in significant resource consumption, such as processor time and memory.
  - It allows for better detection of attacks, particularly through behavioral analysis of software suspected of being infected.

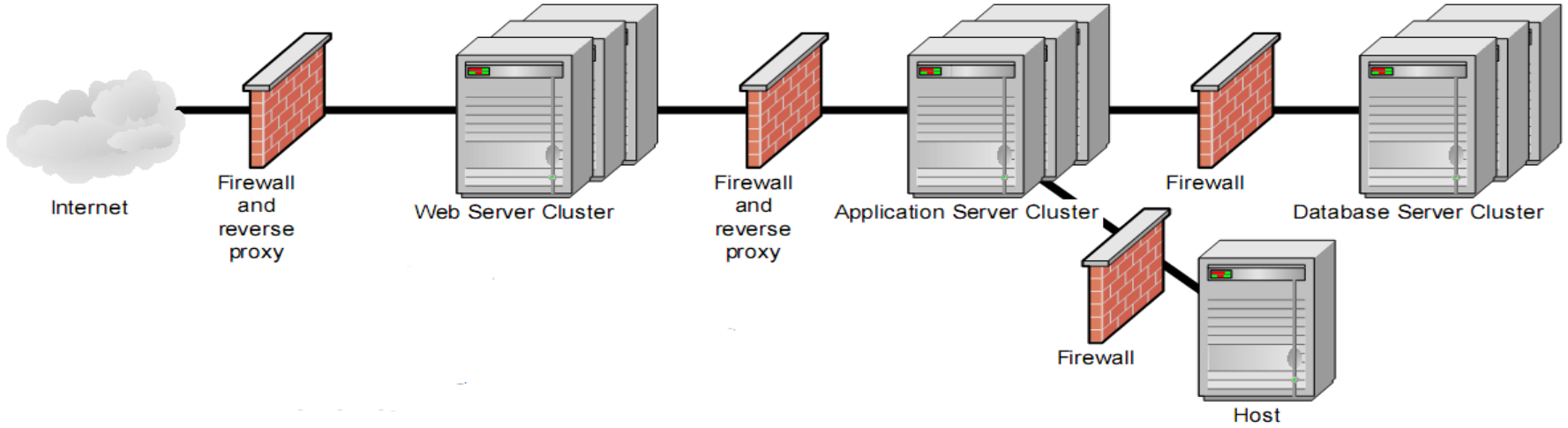
❷Firewall

- an element (software or hardware) of the computer network controlling the communications that pass through it.
- A system that filters network packets to protect access to data accessible through the network as well as to services opened by servers.
- Two types:
  - **Network firewall:** Network equipment that separates the Intranet network from the Internet network.
  - **Personal Firewall:** Protects the workstation

❷Firewall

Example:

Banking Application Architecture



Examples:IPCop, AreaAlarm

❸ Intrusion detection

- Intrusion Detection systems (IDS) are designed to inform, and in some cases to prevent, unauthorized access to or intrusions into the network.
- These systems are also capable of detecting internal hackers (70% to 80% of malicious acts).

❹User training

- Discretion: users' awareness of the low security of communication tools, and of the importance of not disclosing information.
- Virus: Several users opened suspicious attachments ==> staff were regularly informed.
- Charter: requiring employees to read and sign a document outlining their rights and duties, and making them aware of their individual responsibilities.

❺Authentication and encryption

- Authentication is based on 3 principles:
  - Know:login, PSW, …
  - Be :biometrics (fingerprint,…)
  - To have: USB drives, smartcards…

❻Authentication and encryption

- To avoid espionage, we can use digital signature or the **encryption** of all the information.
- Applications:
  - The stored files
  - The transmitted data.