

# cybersecurity

# agenda

- Concepts and definitions
  - What is a cyber attack?
  - Motivation
  - Vulnerabilities and exploits
- Anatomy of a cyber attack
  - The four stages of attack
  - Types of attack
  - Active attacks
    - DDoS, Spoofing, MiTM, ARP attacks, Overflows
  - Passive attacks
    - Wiretapping, Scanning, Phishing and Spear-Phishing, Social Engineering, Worms, Viruses, Trojans, Crypto Attacks
- Zero Day and Advanced Persistent Threats
- Case studies
  - Stuxnet (2009-2011)



# Concepts and definitions

## What is a cyber attack?

A **cyberattack** is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.



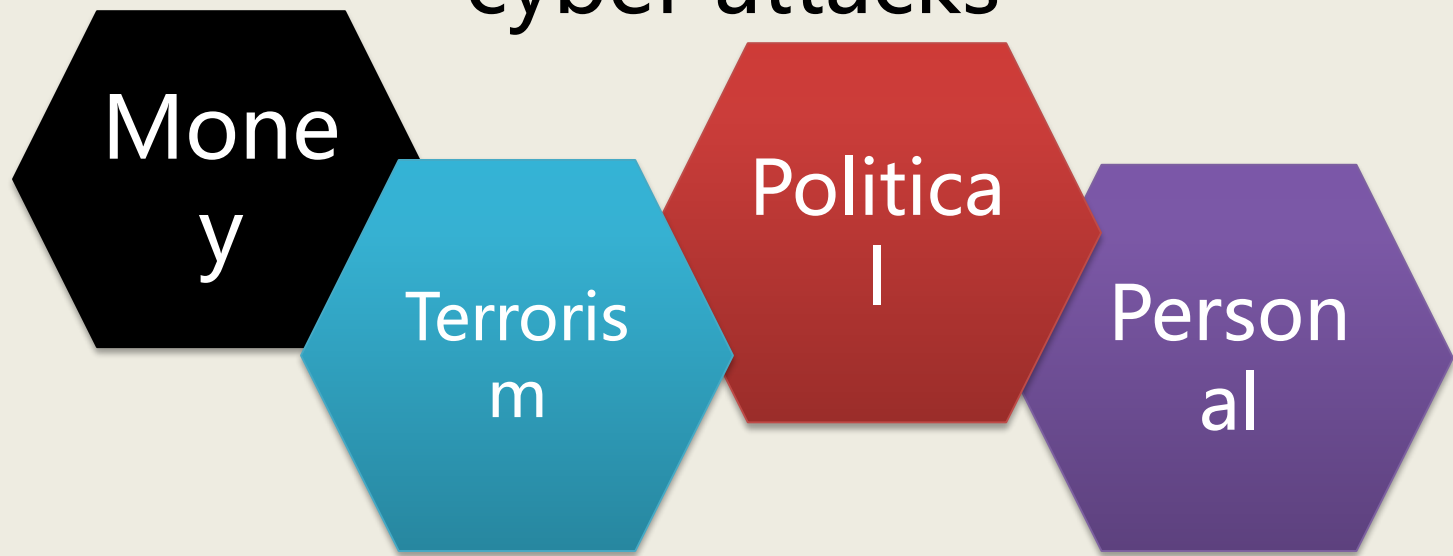
OFF  
ENS  
IVE



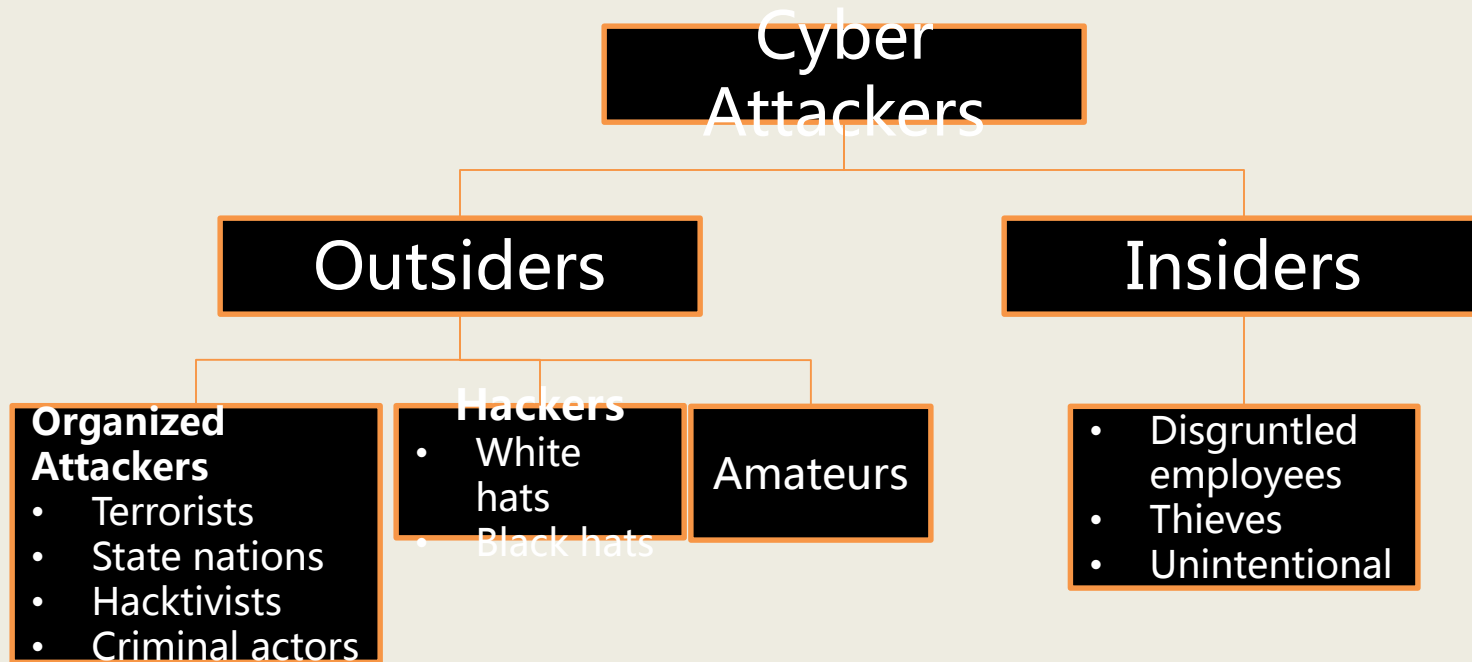
TAR  
GET  
ED

# Concepts and definitions

Understanding the motivation behind  
cyber attacks



# Concepts and definitions

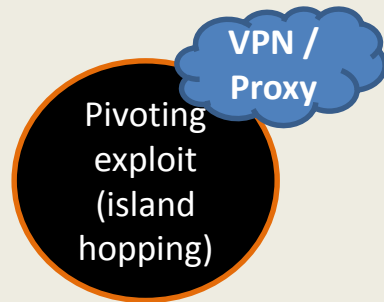
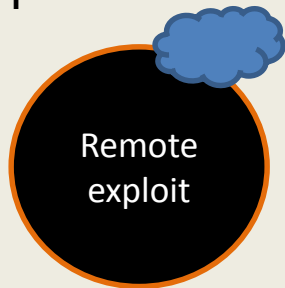


# Concepts and definitions

## Vulnerabilities and exploits

A **Vulnerability** is a weakness in a computer system that can be exploited by an Attacker to perform unauthorized or unintended actions

An **Exploit** is piece of software, chunk of data or sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior in a computer system



# Anatomy of a Cyber Attack

The four stages of an attack

1 - Survey

2 - Delivery

3 - Breach

4 - Affect

Security Perimeter

# Anatomy of a Cyber Attack

## Types of attacks:

(dual taxonomy)

### Outside

Attacker is outside the security perimeter



### Inside

Attacker is 'inside' the security perimeter



### Active

Alters system resources to affect operation

### Passive

Gathers information from the systems but does not alter its state

Where is the attacker located?

**Inside** attackers – foot in the stronghold

**Outside** attackers – looking through the fence

How is the attacker acting?

**Active** – in the system, messing around

**Passive** – looking through the fence, gathering info



# Anatomy of a Cyber Attack

## Active Attacks

## Distributed Denial of Service

Ever been to a music festival? Imagine how would the access gates look like if there weren't any security staff queuing people for ticket validation

**There are three categories of DDoS attacks: volumetric, state exhaustion and application layer**

### Volumetric

- Amplification attacks
- UDP, ICMP, TCPSYN attacks

Attacks:

Application  
**Layer DDoS  
Attacks**

**Advanced  
Persistent  
DDoS**

### Exhaustion

- Loris (Slowloris)
- Http floods

# Anatomy of a Cyber Attack

## Active Attacks

### The issue:

Many TCP/IP protocols do not provide mechanisms for authenticating the source and/or destination of a message

## Spoofing

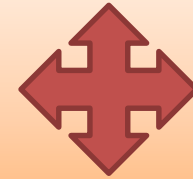
**E-Mail  
Spoofing**

**DNS  
Spoofing**

**IP  
Address /  
ARP  
Spoofing**

**CLID  
Spoofing**

**MAC  
Spoofing**



# Anatomy of a Cyber Attack

## Active Attacks

### Man In The Middle (MiTM)

MiTM attack usually implies one attacker secretly relaying the communication between two parties who believe they are directly communicating with each other.

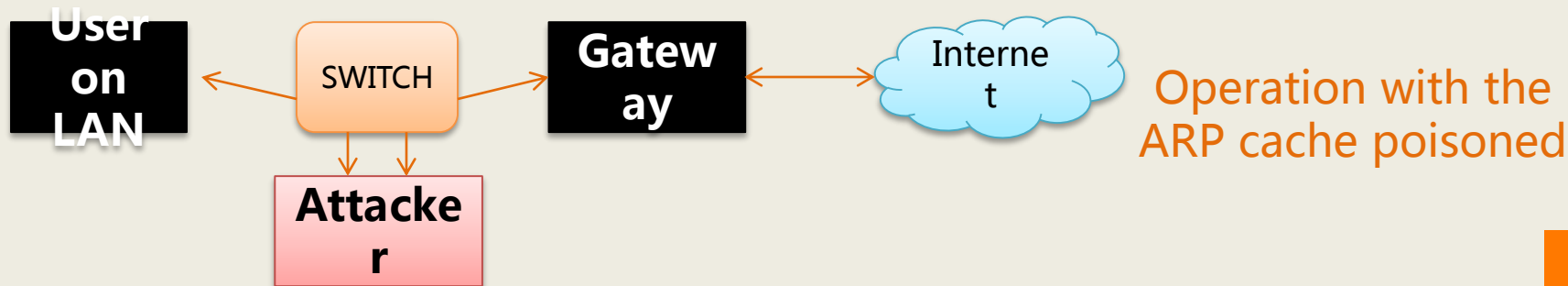


# Anatomy of a Cyber Attack

## Active Attacks

## ARP Attacks

ARP Spoofing (ARP Poisoning, ARP cache poisoning) is a type of attack by which an attacker sends spoofed (forged) **Address Resolution Protocol** (ARP) messages onto a local network, aiming to associate their MAC address with the IP address of another host in order to receive any traffic intended for that IP address

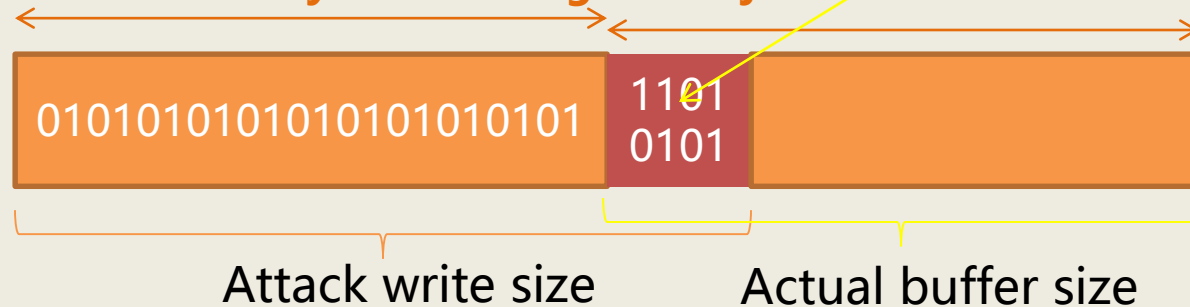


# Anatomy of a Cyber Attack

## Active Attacks

## Overflows – Buffer, Stack, Heap

A buffer overflow is an anomaly in the execution of a program where, while writing data to its buffer, it overruns the buffer boundaries effectively overwriting the adjacent buffer. Malicious executable code

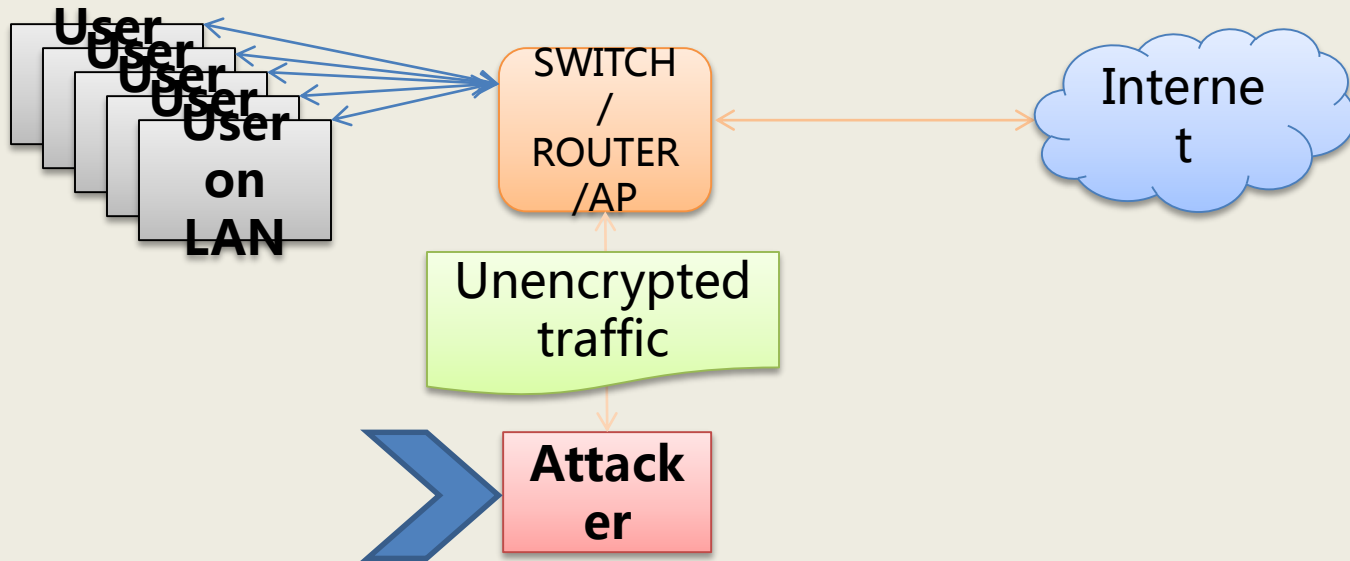


1. Malformed (malicious) program overwrites this buffer (2) with one byte of malicious code
2. That byte of code overwrites executable code located in the next buffer

# Anatomy of a Cyber Attack

## Passive Attacks

Wiretapping, Port Scanning



**Common target:** Unencrypted traffic such as e-mail, application data, application logins, files transferred with FTP etc.)

# Anatomy of a Cyber Attack

## Passive Attacks

## Phishing and Spear-Phishing

**Phishing:** The attempt to obtain sensitive information such as usernames, passwords, credit card details, for malicious reasons, by disguising as a trusted or trustworthy entity

### **Spear phishing**

- directed to specific individuals;
- crafting and delivering of message in such a way as to cater to a specific person or company habits or needs

### **Clone phishing**

- usually by e-mail;
- attacker modifies an existing, legitimate message;
- replaces links with their own;
- spoofs originating e-mail address

### **Whaling**

A type of phishing targeting high-profile executives within business, hoping to gather extremely valuable

# Anatomy of a Cyber Attack

## Passive Attacks

## Phishing and Spear-Phishing





# Anatomy of a Cyber Attack

## Passive Attacks

## Social Engineering

**Social engineering** refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.



# Anatomy of a Cyber Attack

## Passive Attacks

## Worms, Viruses, Trojans

### Worm

- stand alone malicious software
- replicates when executed
- spread itself by copying to other computers in a computer network

### Virus

- malicious software
- it replicates when executed
- modifies other computer programs by inserting own malicious code

### Trojan

- malicious software
- misleads users of its true intent
- deploys payload when executed

# Anatomy of a Cyber Attack

## Passive Attacks

## Cryptomalware / Ransomware

**Cryptomalware:** type of malware that threatens to disclose or disable access to user's data by encrypting it with a public/private key pair.

**Ransomware:** a type of cryptomalware that will disable access to data unless a ransom is paid, usually in the form of untraceable



# Anatomy of a Cyber Attack



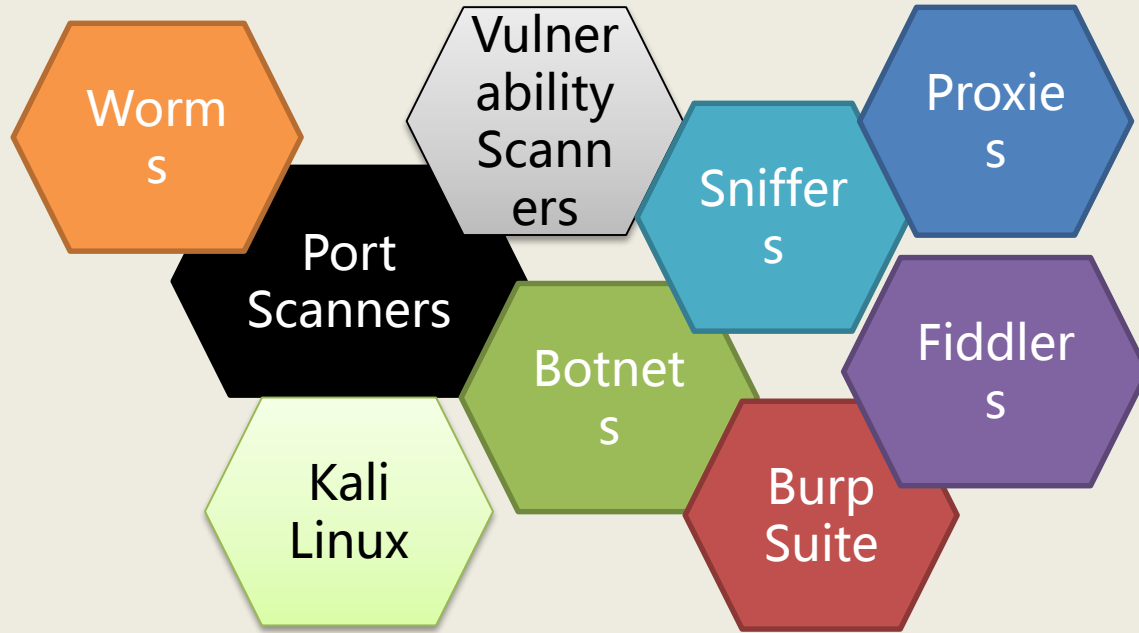
# Anatomy of a Cyber Attack

An **advanced persistent threat** is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity.

The "**persistent**" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack

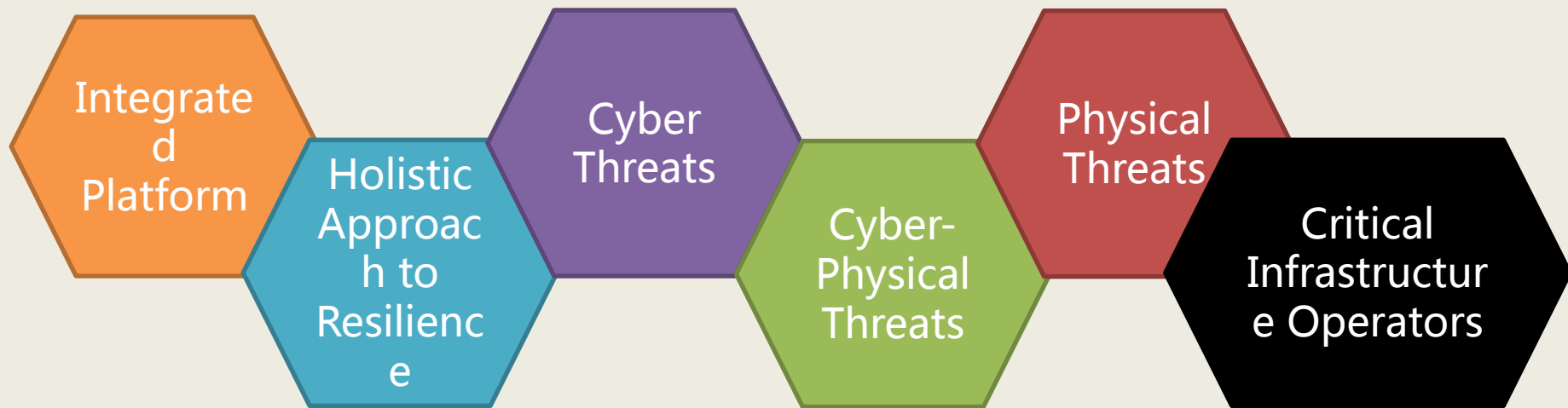


# Anatomy of a Cyber Attack



Tools of the trade

# Enhancing Resilience



Horizon 2020 Project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786409



# Anatomy of a Cyber Attack



Cyber attacks are growing in number, complexity and impact

Attackers have various motivations ranging from personal to political

Attacks are becoming more difficult to mitigate as more advanced forms appears

State-actors are increasingly using cyber-weapons for their geo-political agendas

Prevention requires both awareness AND threat Intelligence

Key Take aways



# Case studies: STUXNET

Stuxnet is a malicious computer worm, first uncovered in 2010. Thought to have been in development since at least 2005, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program. Although neither country has openly admitted responsibility, the worm is believed to be a jointly built

## Timeline American/Israeli cyberweapon

**2006** – First piece of code compiled specifically to target industrial PLCs

**2007** – Conficker appears and starts spreading

**2009** – Attackers begin deploying Stuxnet to Iran using Conficker as a infection vector

**2010** – Security firm VirusBlokAda identifies Stuxnet as malware, after reviewing a sample from Iran

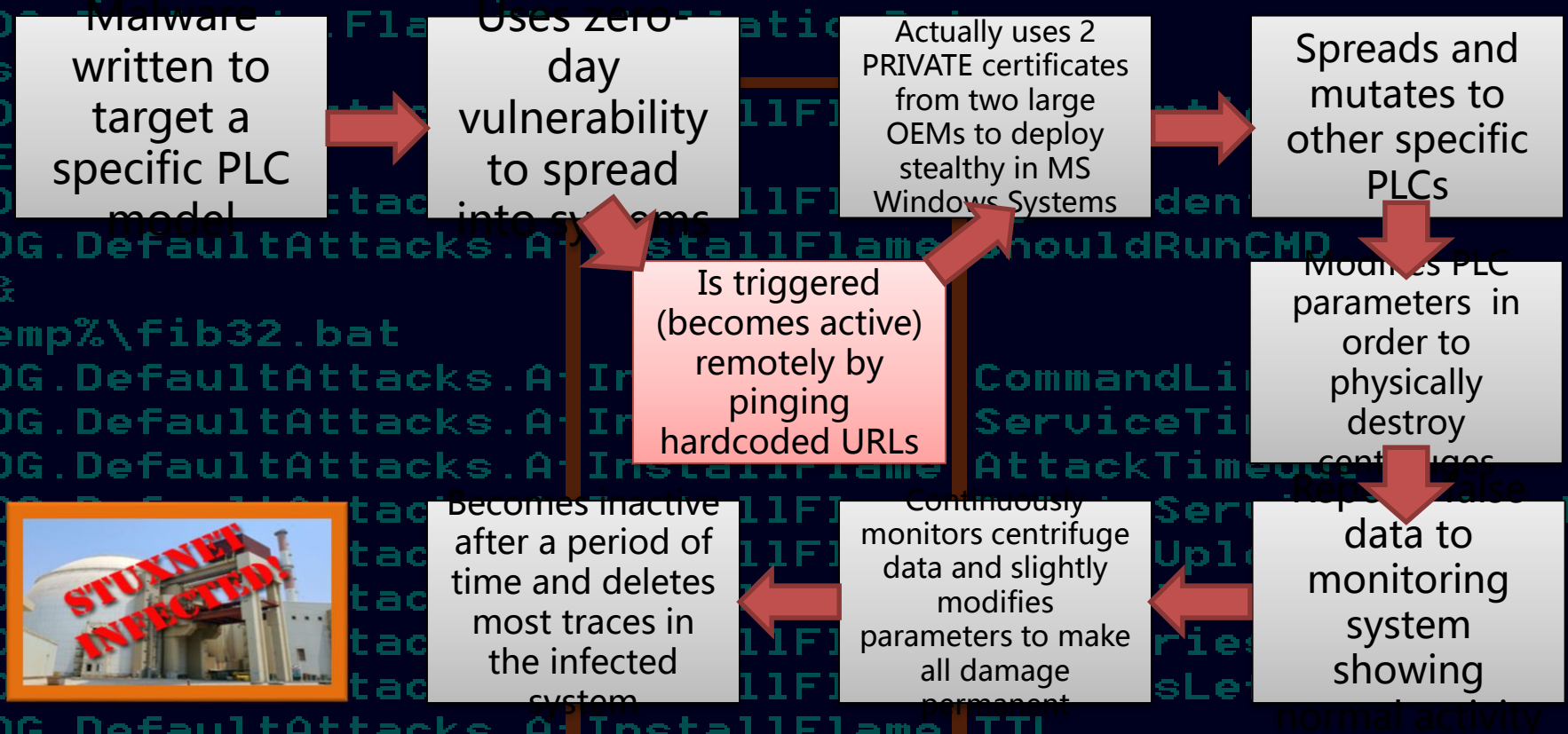
**2010** – Iranian President Mahmoud Ahmadinejad admits that a cyber weapon had damaged gas centrifuges at a uranium enrichment facility

1<sup>st</sup> time a malware attacks industrial components

1<sup>st</sup> time a malware targets specifically a type of physical equipment

1<sup>st</sup> time a malware is believed to have been built by state-actors

# Case studies: STUXNET



# Quick Recap

1. What is a cyber attack?
2. What drives the attacker?
3. What are the stages of attack?
4. What are the types of attack?
5. The usual suspects
6. The newcomers
7. When things go wrong (case study)

Thanks 😊