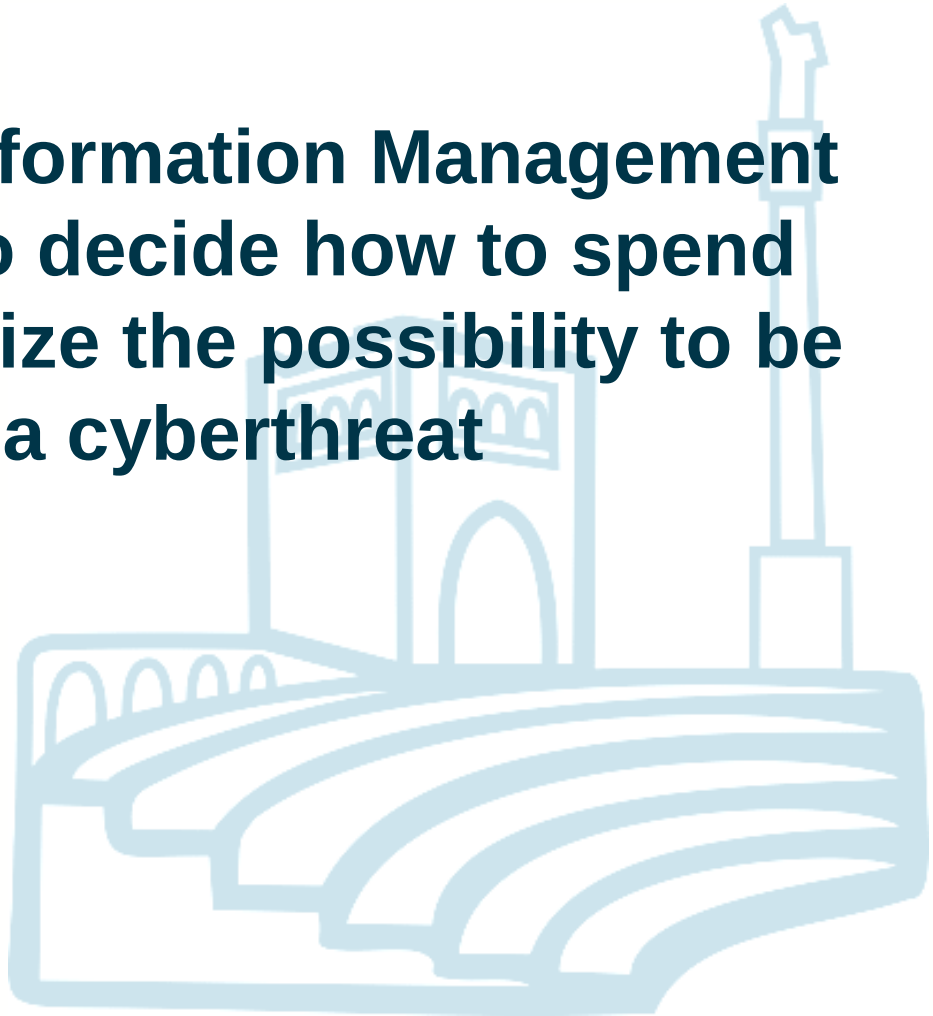
CyberSecurity Fundamentals

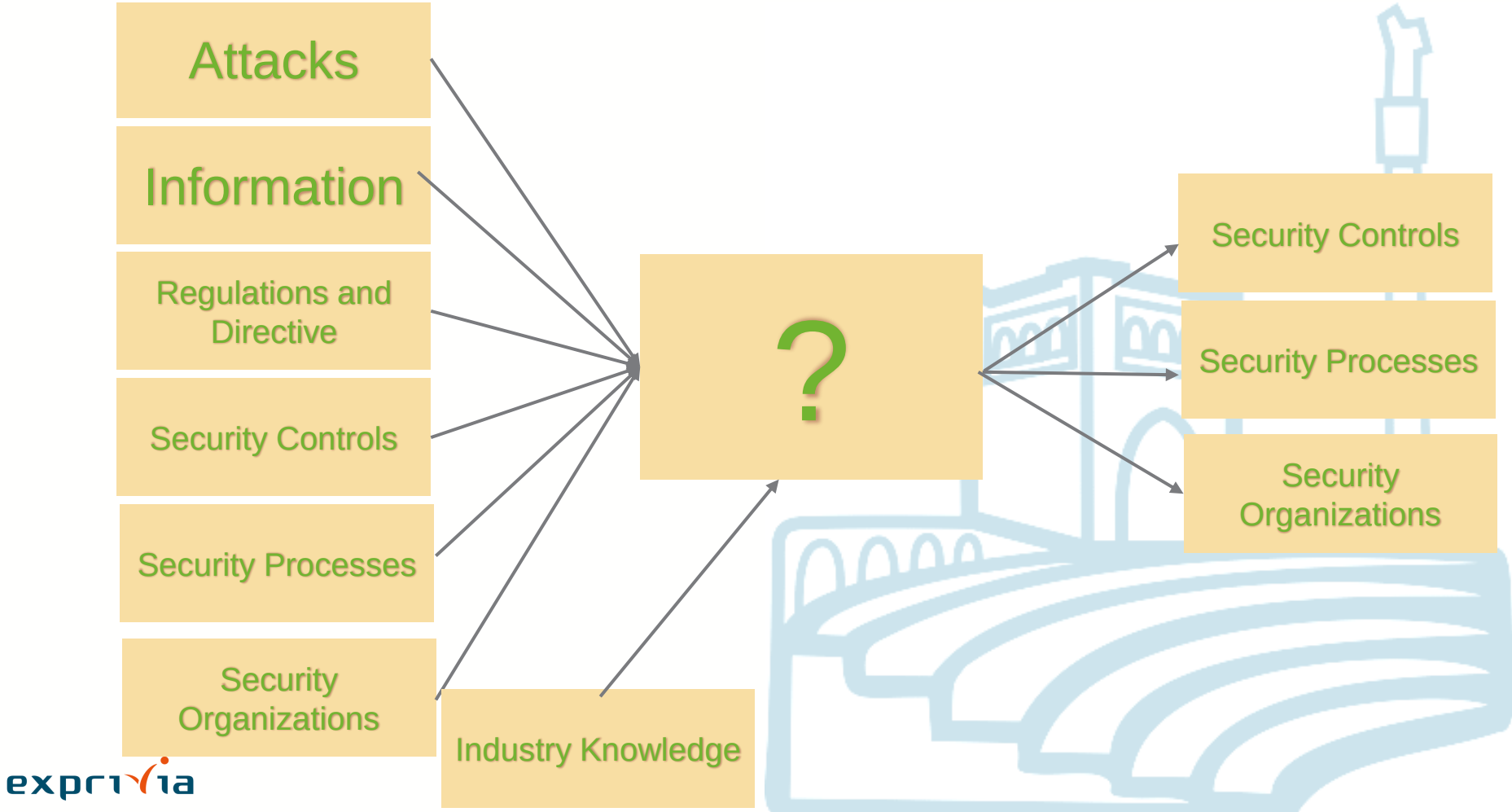
@domenicoraguseo

Nov, 2021

Security Information Management is the art to decide how to spend .01$ minimize the possibility to be a victim of a cyberthreat



exprivia

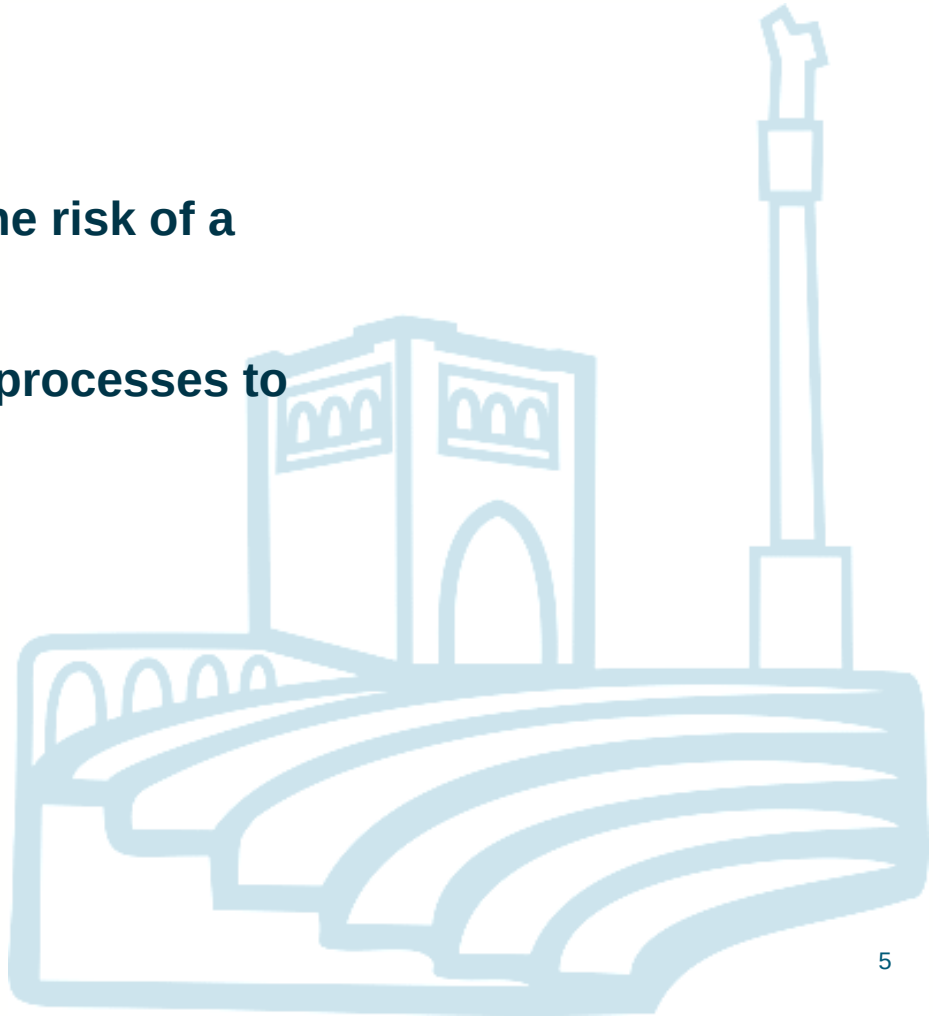

Attacks
Information
Regulations and Directive
Security Controls
Security Processes
Security Organizations
Industry Knowledge
?
Security Controls
Security Processes
Security Organizations

Cosa vuol dire che la sicurezza è un bene dal valore intrinseco

Non può essere calcolato ROI

Agenda

- Attacks and Kill Chains
- Security Controls
  - Activities to be done to mitigate the risk of a cyber-attack
- Security Processes
  - Security controls orchestrated in processes to produce consistent results
- Organizations to execute processes
- Technologies used by Organizations
  - Qradar
- Information
- Industry Knowledge



Changes in Enterprise: Security Challenges are impacting innovation

External threats

Sharp rise in external attacks from non-traditional sources

- Cyber attacks
- Organized crime
- Corporate espionage
- State-sponsored attacks
- Social engineering

Internal threats

Ongoing risk of careless and malicious insider behavior

- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employee actions
- Mix of private / corporate data

Compliance

Growing need to address an increasing number of mandates

- National regulations
- Industry standards
- Local mandates

Impacting innovation

Mobility

Cloud / Virtualization

Social Business

Business Intelligence

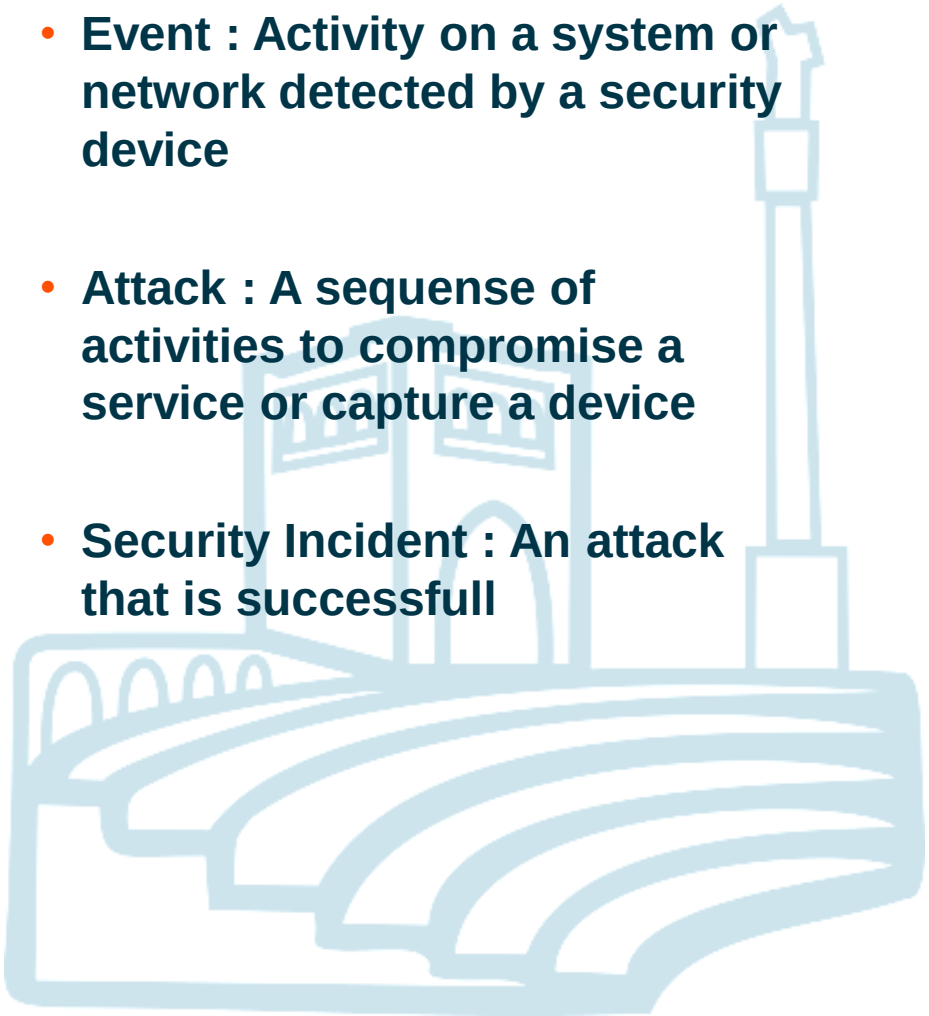
exprivia

Attacks

- SQLi
- CIA
- Code Injection
- Disenfranchaising
- Brute Force
- Undefined
- Physical Access
- Heartbleed
- XSS
- BEC
- Spoofing

- APT
- Ransomware
- Misconfiguration
- Malvertising
- Malware
- Watering hole
- Phishing
- DoS and DDoS
- Spectra/Meltdown
- Dridex and Redirection Attack

- Event : Activity on a system or network detected by a security device
- Attack : A sequense of activities to compromise a service or capture a device
- Security Incident : An attack that is successfull

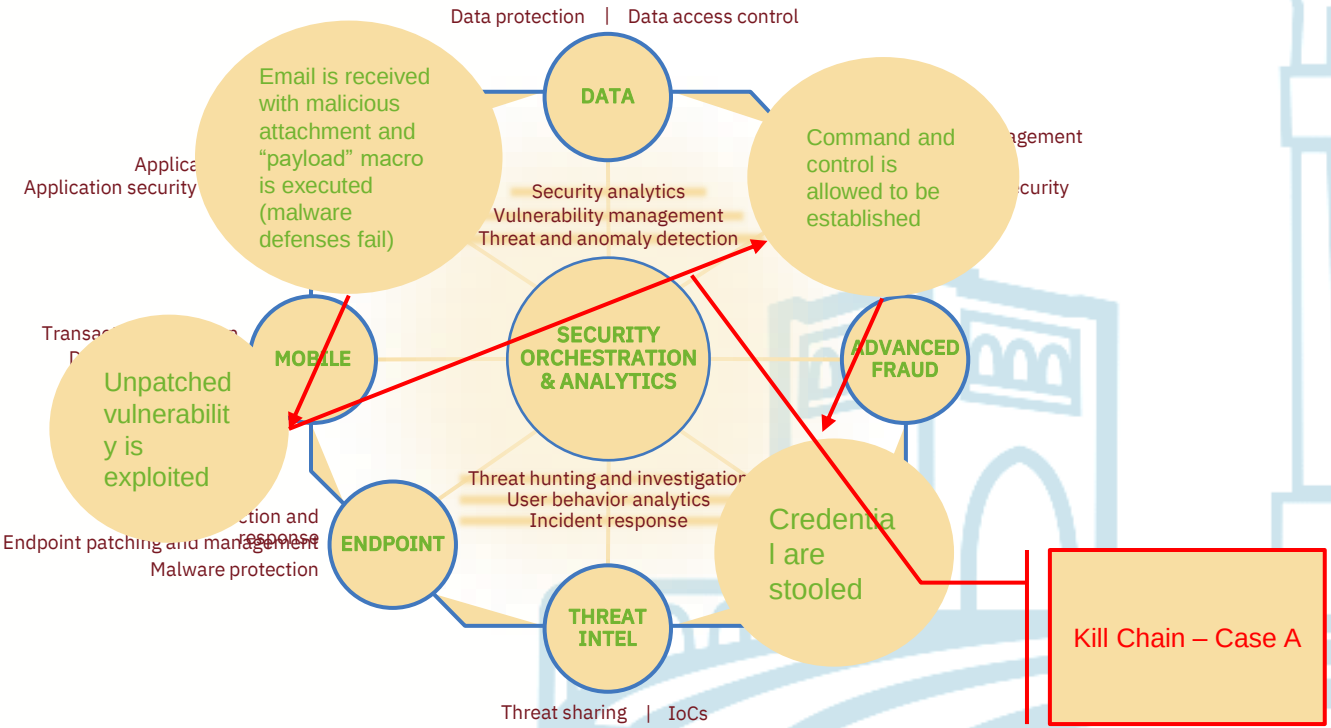


Kill Chain

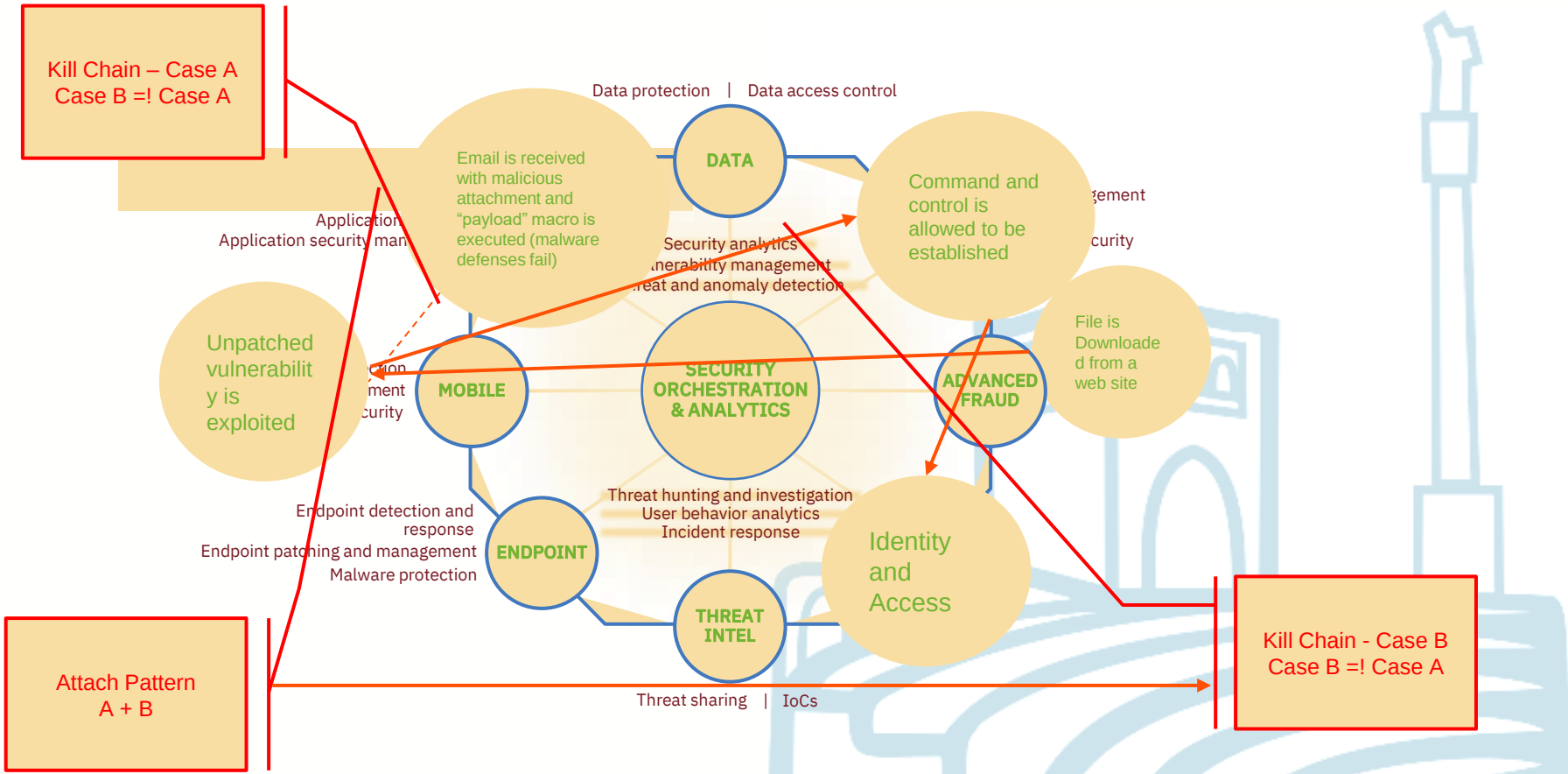
- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objective

- Offering
- Development
- Go to marketing
- Testing
- Development
- Operation
- Financial

Activities performed during Business Email Compromise – Case A

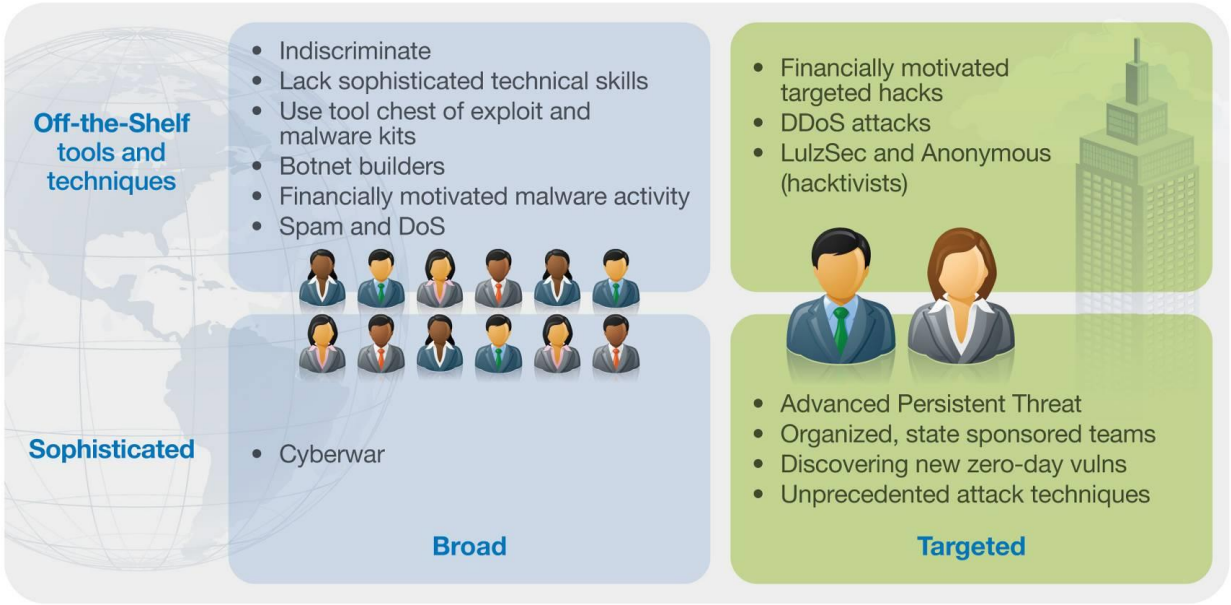


Watering hole .. A change in attach strategy . Case B



exprivia

Who is attacking our Networks?



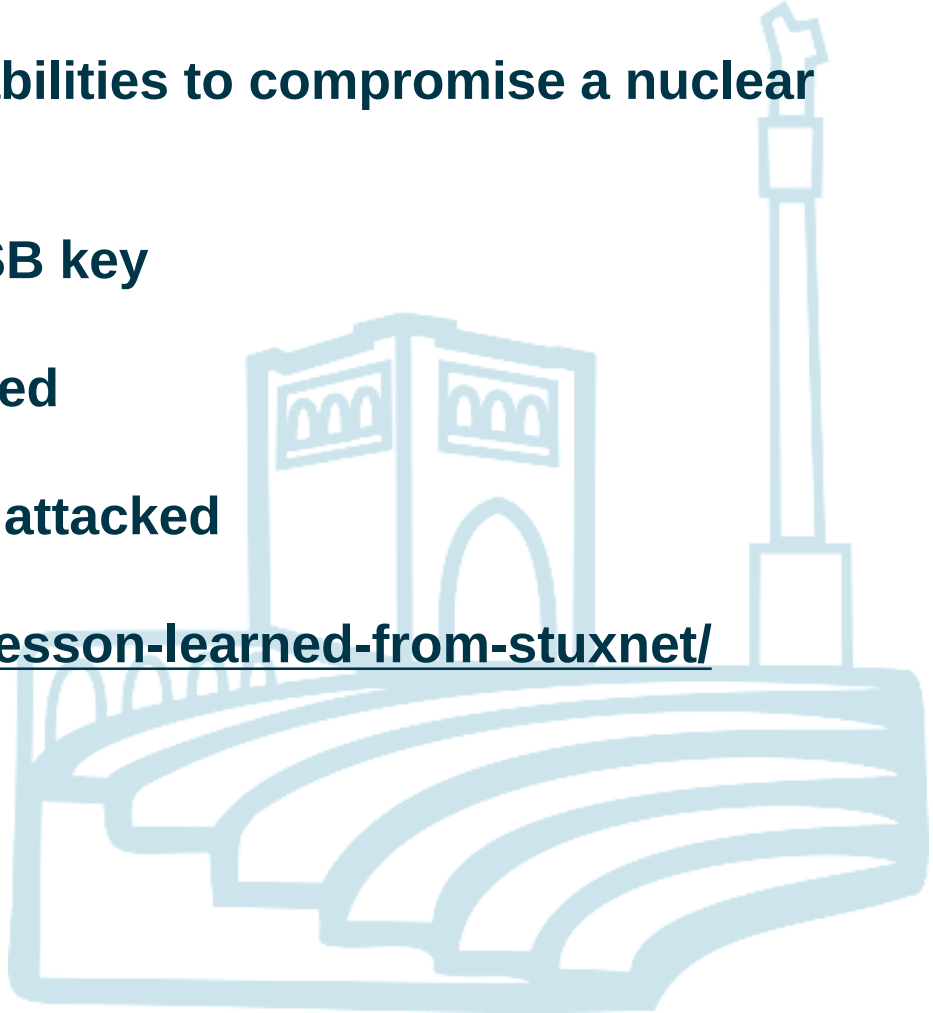
Source: IBM X-Force® Research and Development

Mirai

- Malware that transforms devices with Linux into bots
- These botnets can be used for network attacks including DDoS
- Main target is IP cameras and home routers
- Mirai sourcecode can be found online in open forums
- Date: August – October 2017
- Devices continue to work normally
- IoT needs to be secure
- Security as an ‘instrinsic value’
- Impact depends on how digitalised the enviroment is
- Interesting readings: https://securityintelligence.com/2016-the-year-of-the-ddos-attack/
- Interesting readings: https://securityintelligence.com/the-future-of-cybersecurity/

Stuxnet

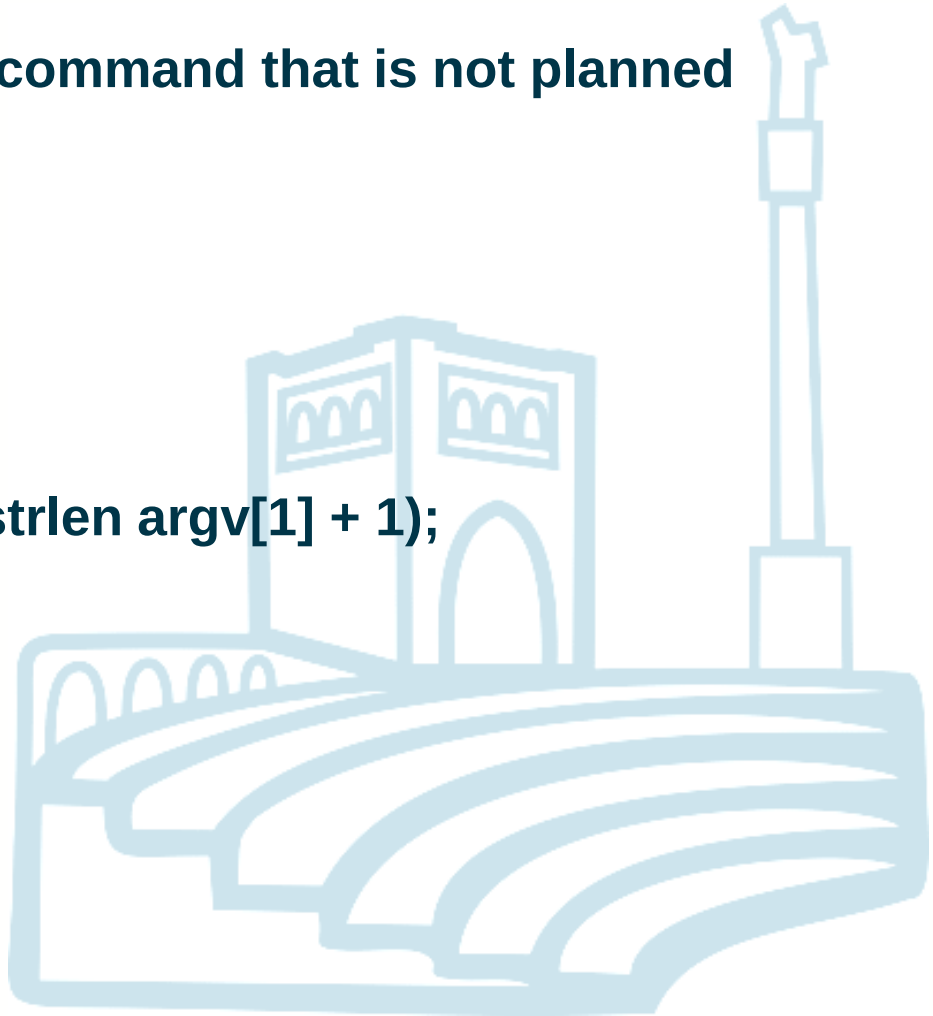
- Malware used 4 windows vulnerabilities to compromise a nuclear plant
- Malware infected the plant via USB key
- SCADA enviroments are not closed
- Even closed enviroments can be attacked
- https://securityintelligence.com/lesson-learned-from-stuxnet/



CMDi = Command Injection

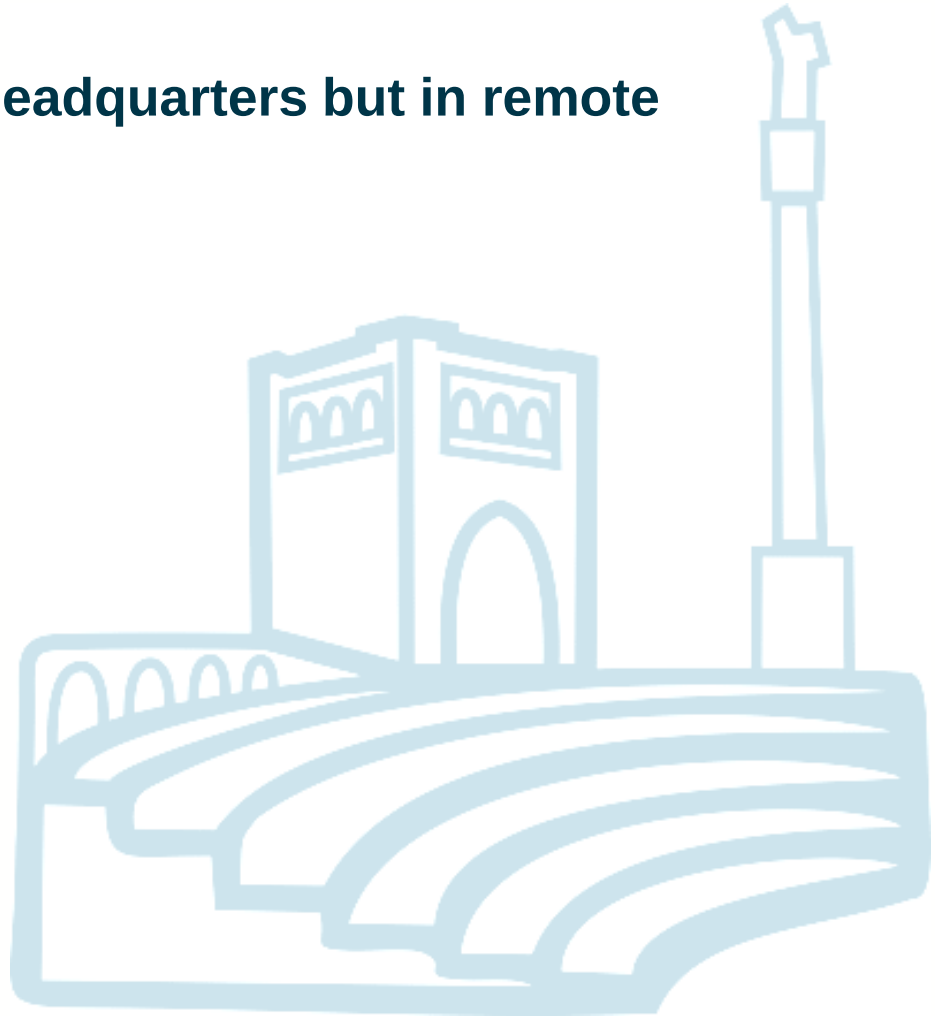
Force the application to execute a command that is not planned

```
#include <std.io>
#include <string.io>
int main (int argc, char ** argv) {
char hello [] = ‘hello’;
char* command;
Command = malloc ( strlen(hello) strlen argv[1] + 1);
System (command)
 }
```



Disenfranchaising

Attack enterprise not in principle headquarters but in remote branch of office



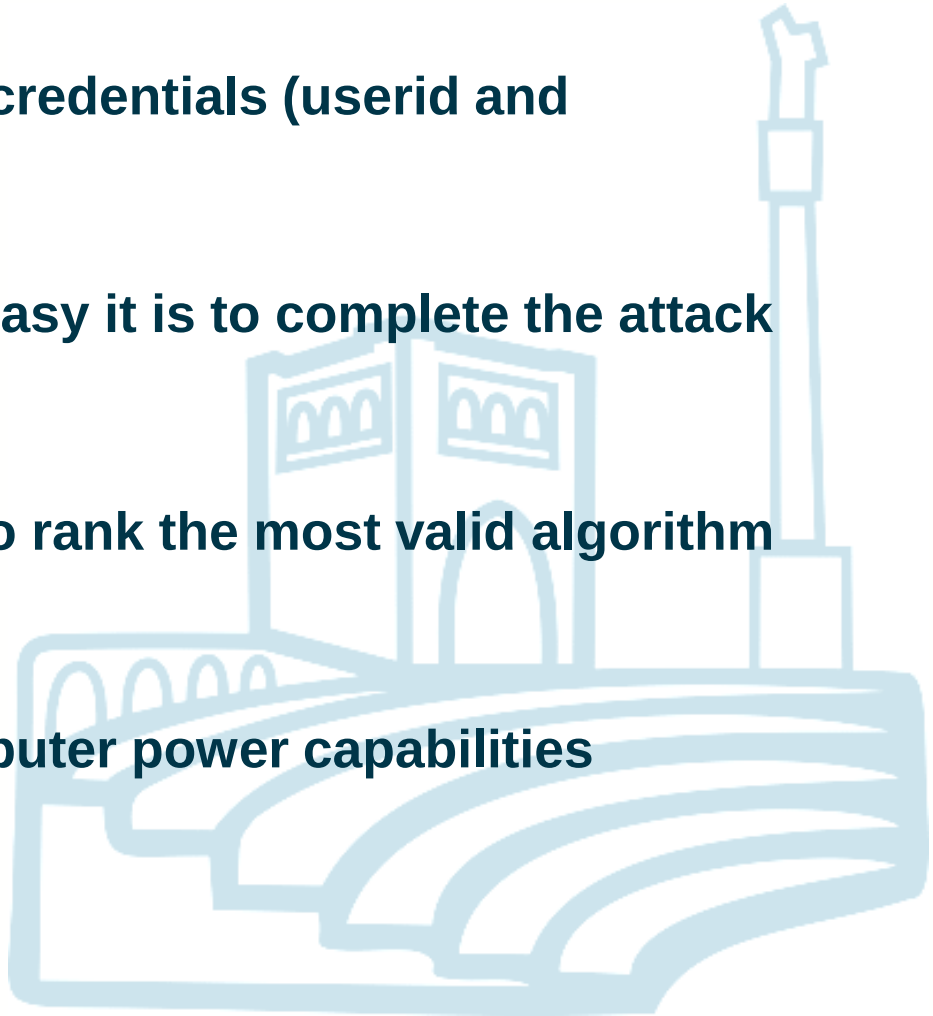
Brute Force

Trying all possible combinations of credentials (userid and password) to gain access

More info we make available, more easy it is to complete the attack successfully

Brute Force Search uses analytics to rank the most valid algorithm to identify the password

Increasing with the increase of computer power capabilities

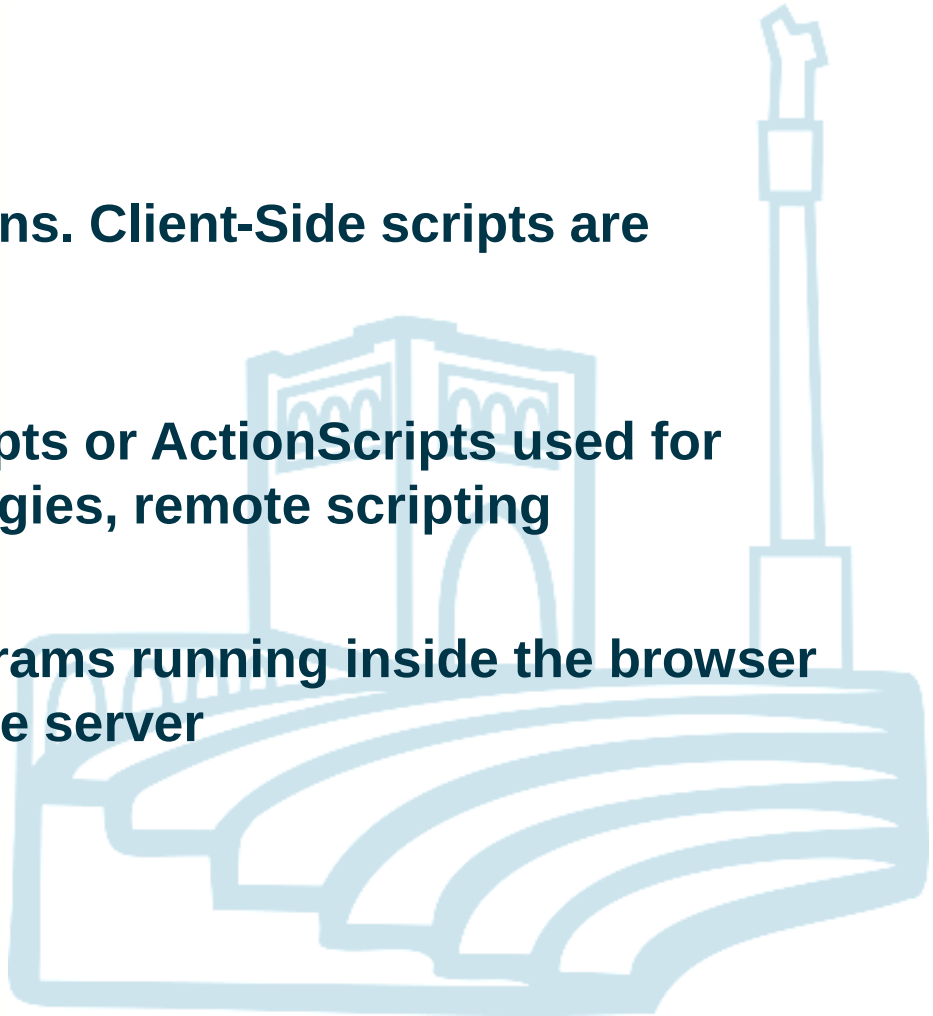


Undefined

Attack is noticed but it is not clear who is attacking who

XSS = Cross Site Scripting

- Usually Impacts Web Applications. Client-Side scripts are inserted into web pages
- Client-Side scripts are JavaScripts or ActionScripts used for Dynamic HTML, Flash Technologies, remote scripting
- Remote Scripting is about programs running inside the browser to exchange information with the server



Ransomware

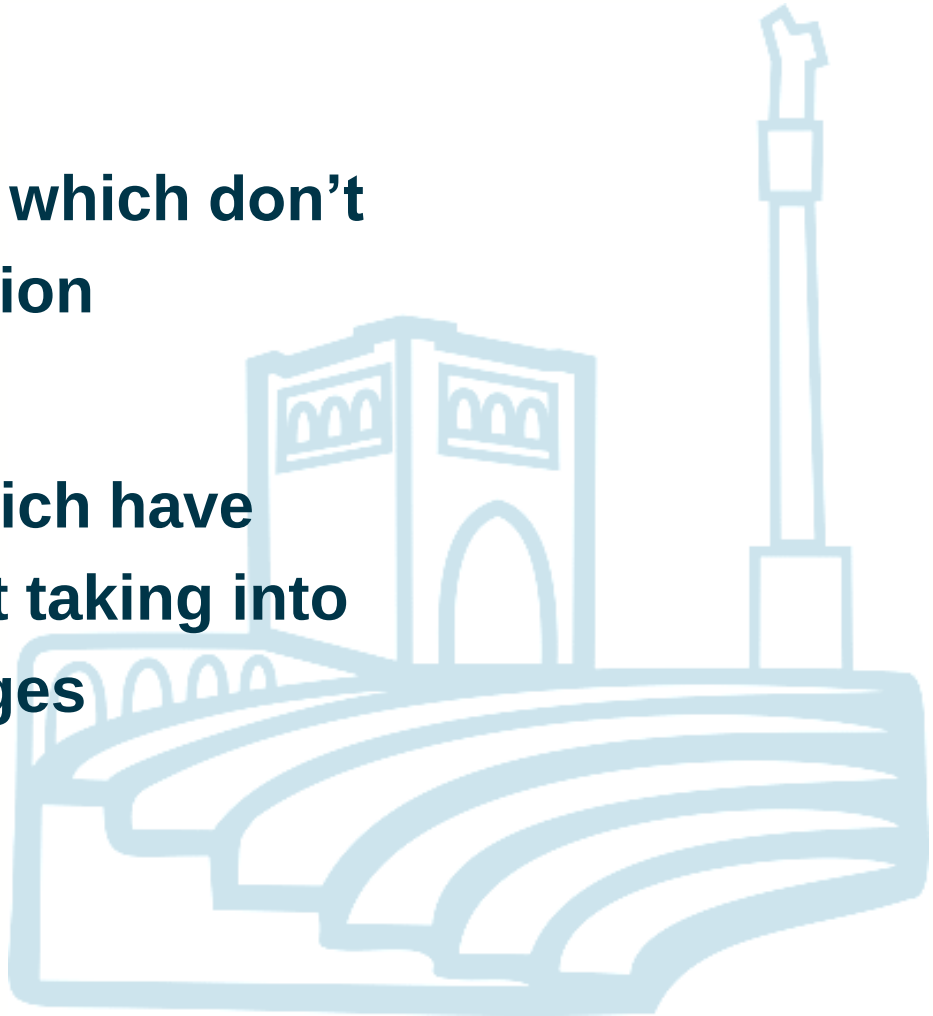
- **Make the service unavailable and ask ransom to restore the service**

- **Criminal behaviour is associated to cryptolcker but it is used also to hook the access of the service**

Misconfiguration

- **Hardware and /or software which don’t have the proper configuration**

- **Hardware and software which have been upgraded but without taking into consideration all the changes**

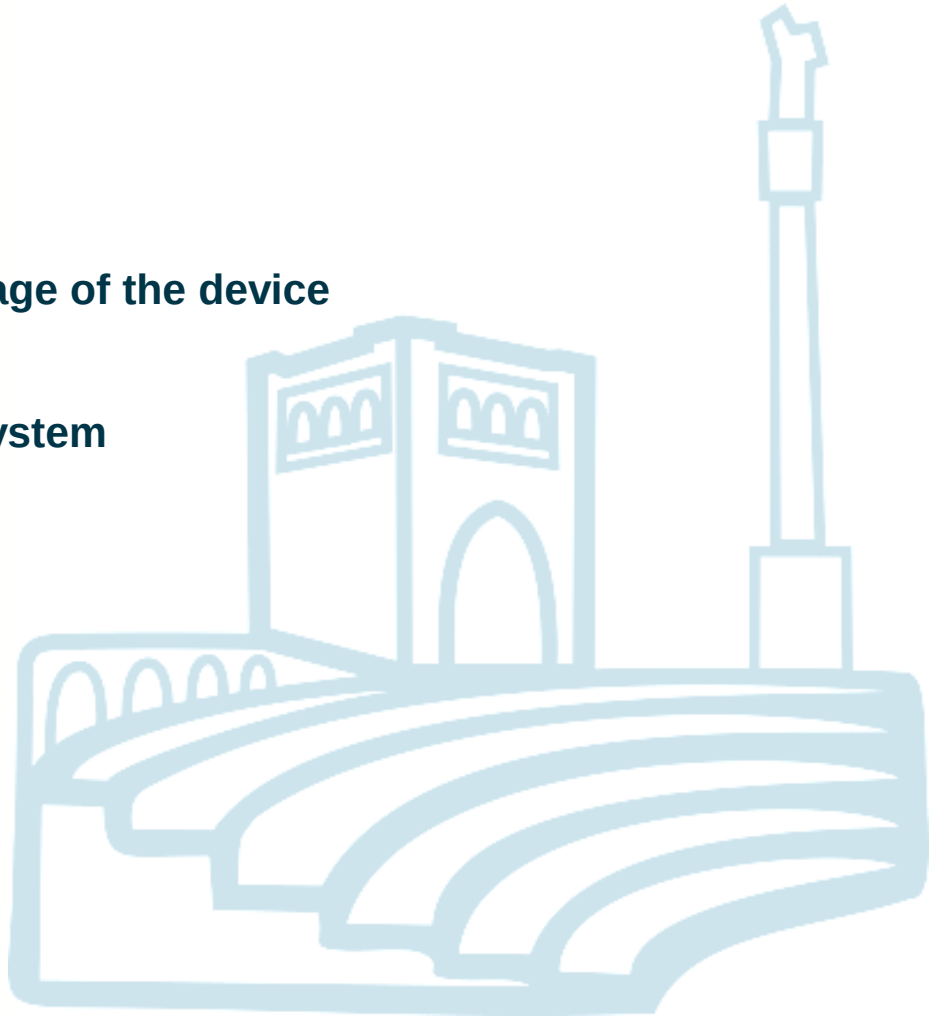


Malvertising

- **Framework used to distribute malware through marketing campaigns (online...)**

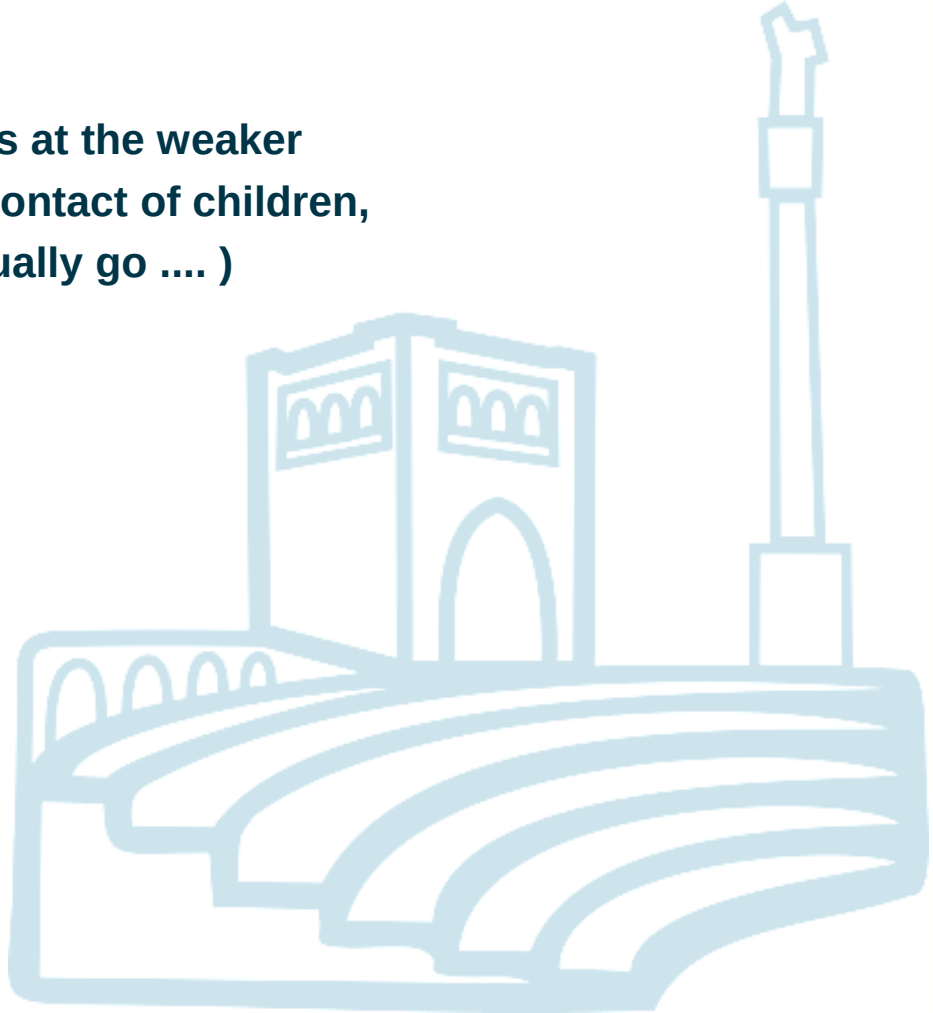
Malware

- Malicious software
- Software used to disrupt the normal usage of the device
- Gather information, access computer system
- Display unwanted advertisment
- Evolution of Virus



Watering Hole

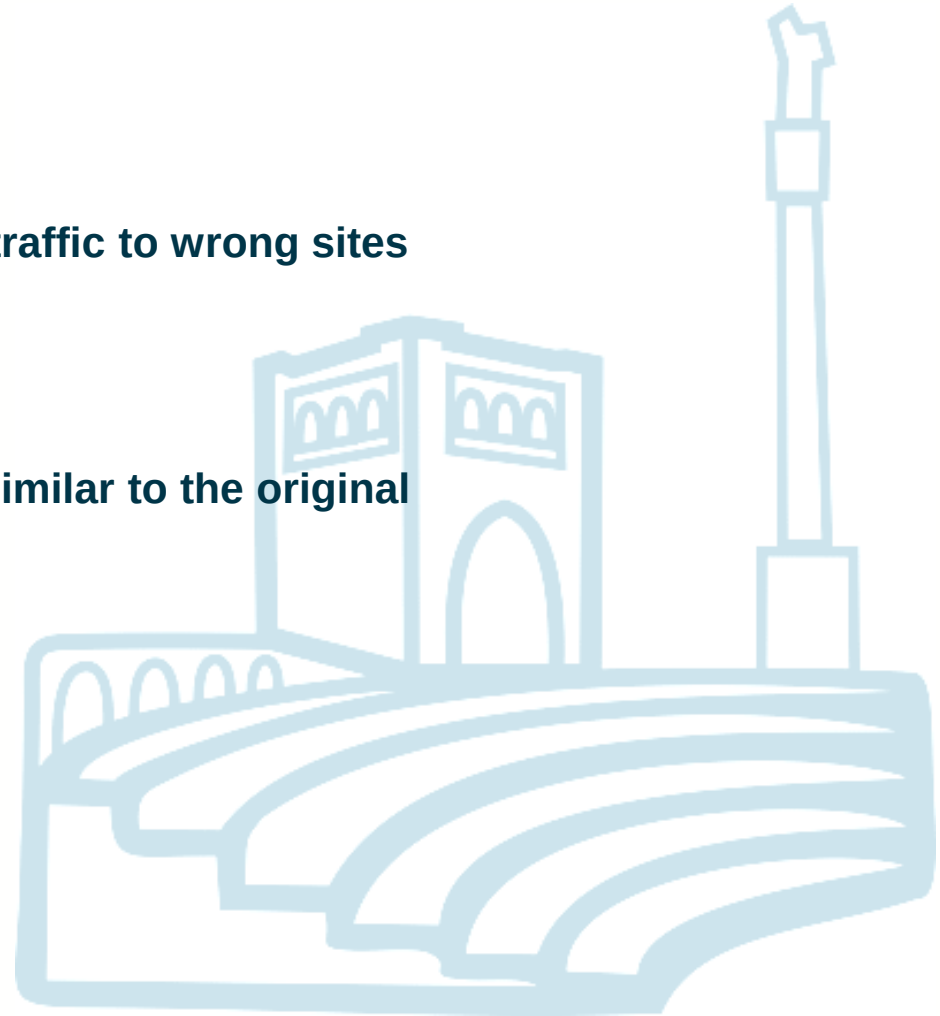
Does not attack the target directly, but looks at the weaker element of the chain (e.gvc the fb contact of children, the hotspot of the restaurant where you usually go ....)



exprivia

Dridex and Redirection Attach

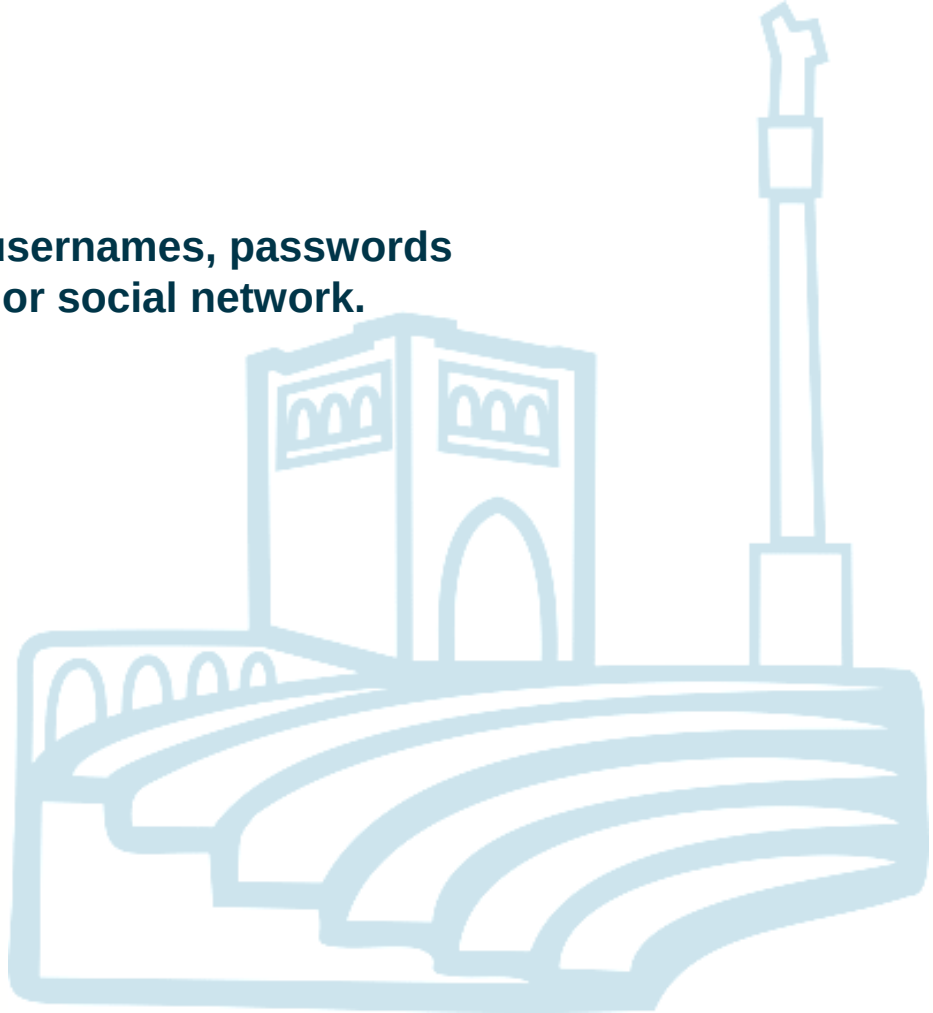
- The general idea is to redirect all the traffic to wrong sites
- DNS poisoning
- Traffic redirected towards sites very similar to the original one



Phishing

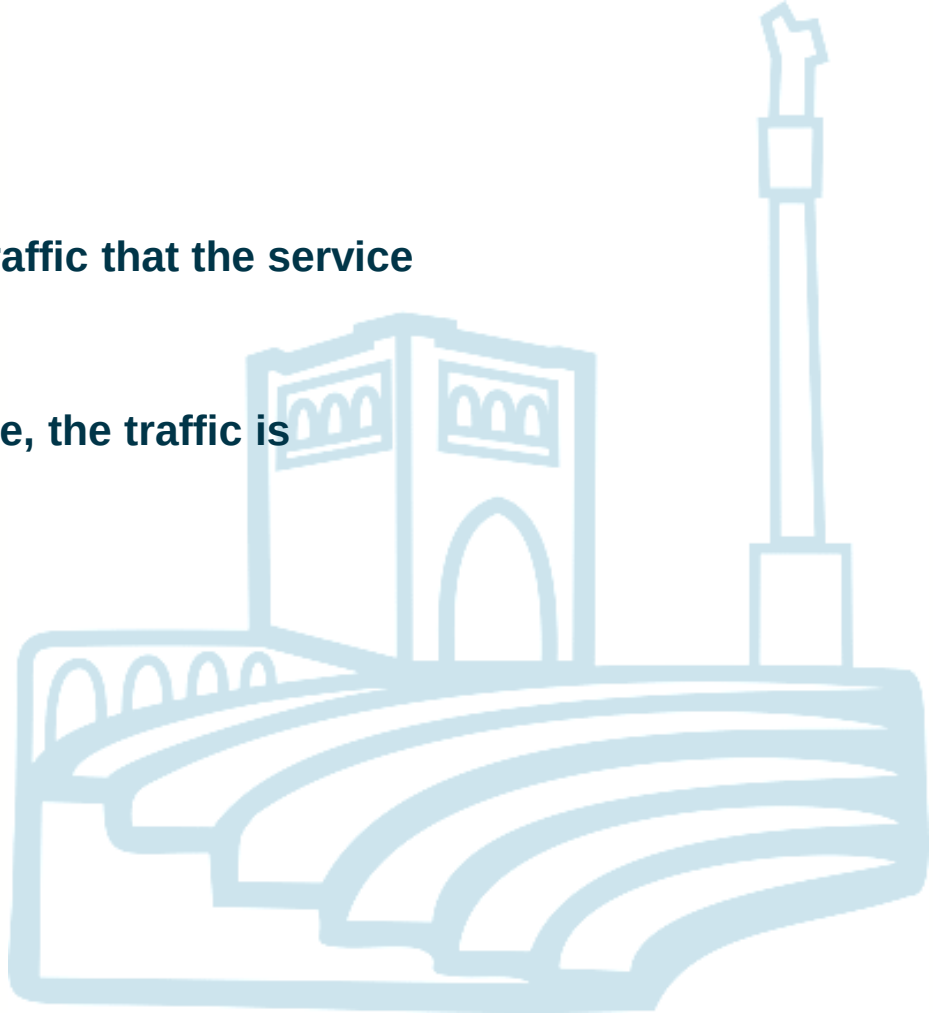
- Obtaining sensitive information (e.g usernames, passwords ..... Credit card details) with an email or social network.

- Instant messaging



DDoS

- Deny of Service by creating a specific traffic that the service is not able to sustain
- DDoS means Distributed Deny of Service, the traffic is generated by multiple points
- 100 Gbps



Business Email Compromises

1) Hacker via phishing an executive gain access to inbox, or emailing employees from a domain and giving the feeling that the email is received by an executive spoofing

2) Hacker has usually 5 options :

CEO Fraud, where CEO sends email to an employer

Request to change the payment

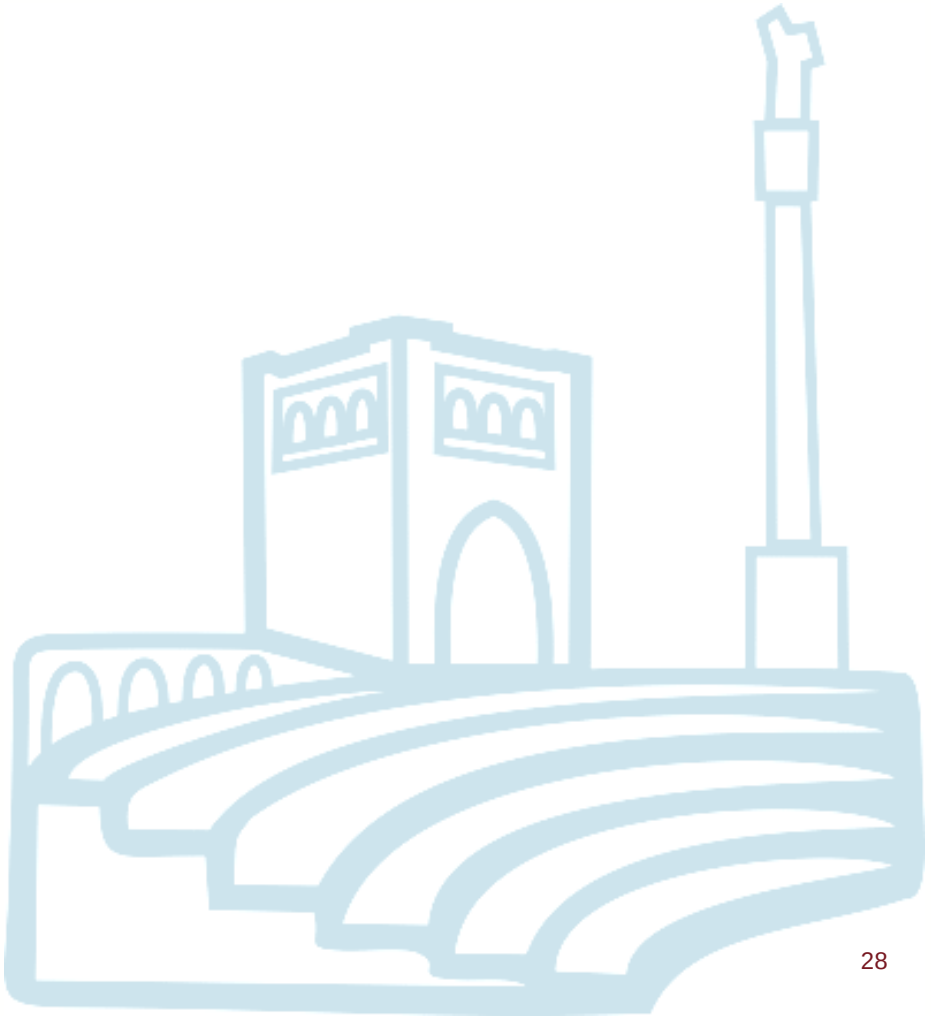
Attorney impersonation

Account compromise

Data theft

exprivia

Information



Information on CyberCrime

Cybercrime reports

Clusit

https://clusit.it/rapporto-clusit/

Libro Bianco

https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco

Exprivia Threat Intelligence

https://www.exprivia.it/it/238/cybersecurity-ottimizzare-gli-investimenti-per-ridurre-il-rischio-complessivo.php

Blog

@domenicoraguseo

@Exprivia_CY

Personalized reports

https://csirt.exprivia.it/

exprivia

Vulnerabilities

- CVE : http://cve.mitre.org/about/faqs.html
- CVSS : https://www.first.org/cvss/user-guide?cm_mc_uid=42896661542614867760237&cm_mc_sid_50200000=1493722532

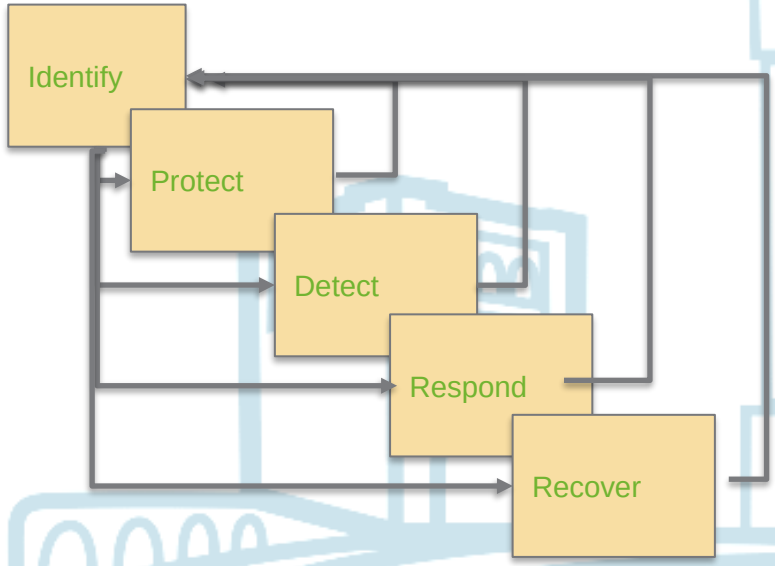
Security Controls

Security Controls

- Italian Security Framework
- https://www.cybersecurityframework.it/

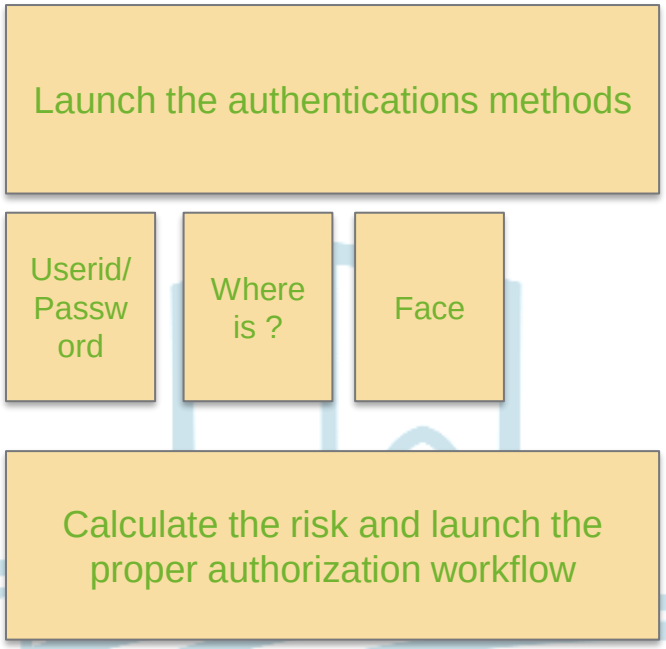
- Minimal Security Control Mandatory for the PA
- https://www.agendadigitale.eu/sicurezza/le-misure-minime-di-sicurezza-ict-per-la-pa-cosa-sono-e-come-applicarle/

- Critical Security Controls
- https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf



Access Management

- Provide secure access for authenticated users inside and outside of your enterprise with proactive policies
- Single Sign-On / Portfolio
- Authentications
  - What you know, have, are
    - Multi-Factor authentication
    - Strong Authentication
    - Step-up Authentication
- Risk Based Approach
- Front end needs to assess the risk
- Back end need to activate workflow based on risk



Security Processes

Security Processes

- Security controls need to be orchestrated in processes to provide consistent results
- CSIRT frameworks are a set of process and services necessary for preventing detecting and reacting to an attack

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://www.first.org/resources/guides/

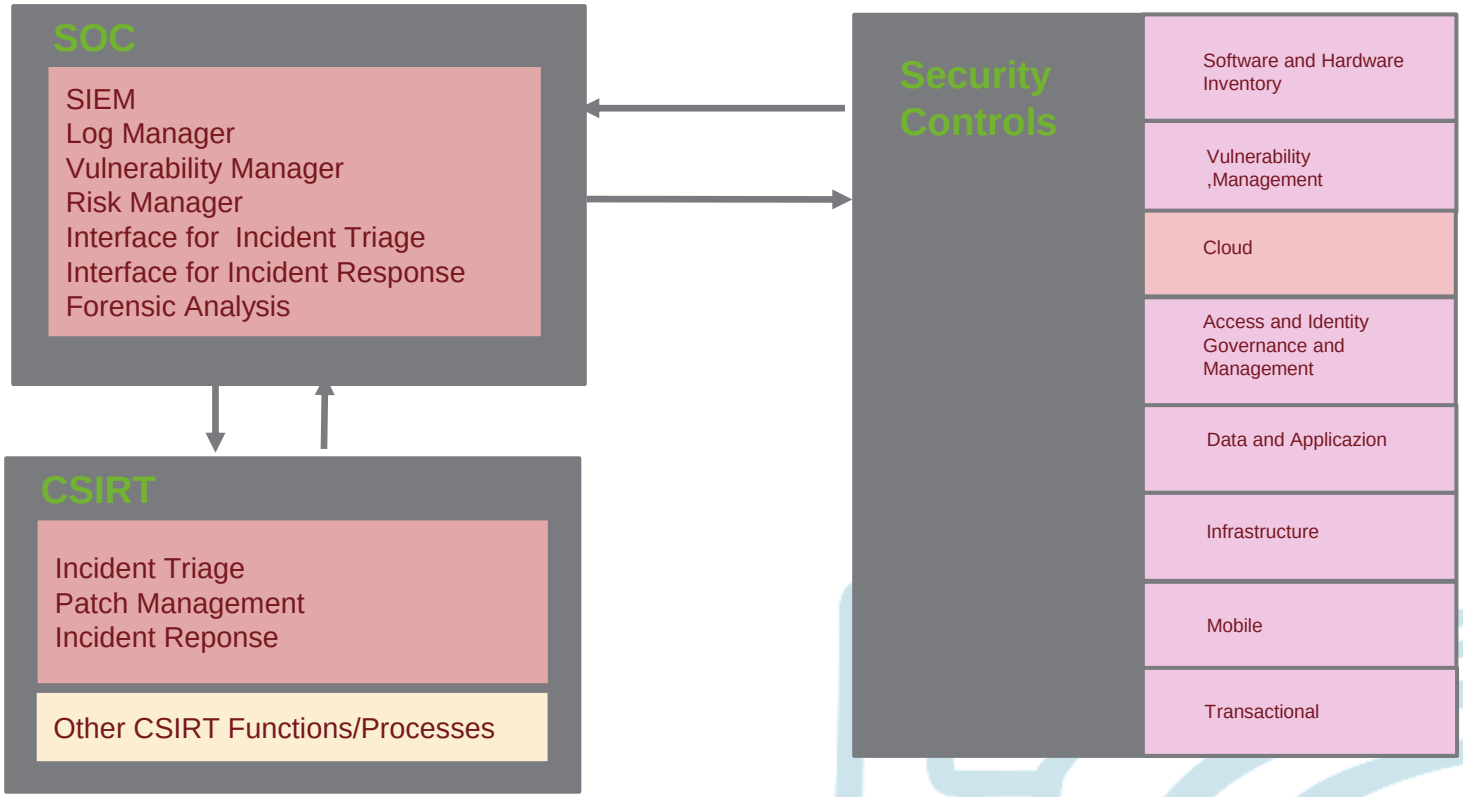
http://www.cert.org/incident-management/csirt-development/cert-authorized.cfm?

Cosa vuol dire strong authentication

Diversi tipi di autenticazione vengono utilizzati per calcolare il rischio dell'accesso

Security Organizations

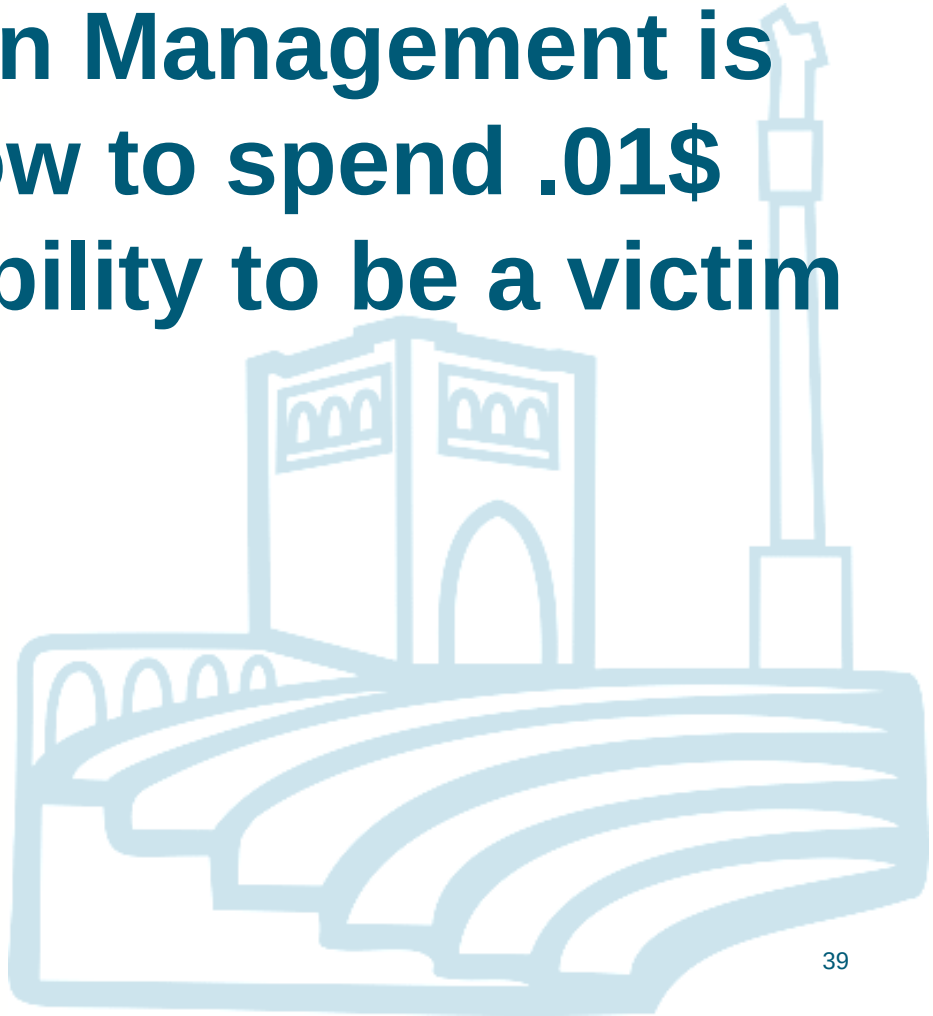
Organizations supporting CSIRT processes



expriv ia

Security Information Management is the art to decide how to spend .01$ minimize the possibility to be a victim of a cyberthreat ?

YES



What is an attack ?

A sequense of activities to compromise a service or capture a device

What is a security incident ?

An attack that is successfull

Threats are always External

Attacks can be internal and external

Stuxnet is an external attack or an internal

It depends

Stuxnet is an external attack or an internal

It depends

CSO need to invest to reduce the risk of an attack or to be compliant to directives and regulations ?

Both

Kill chain

Reconnaissance

Weaponization

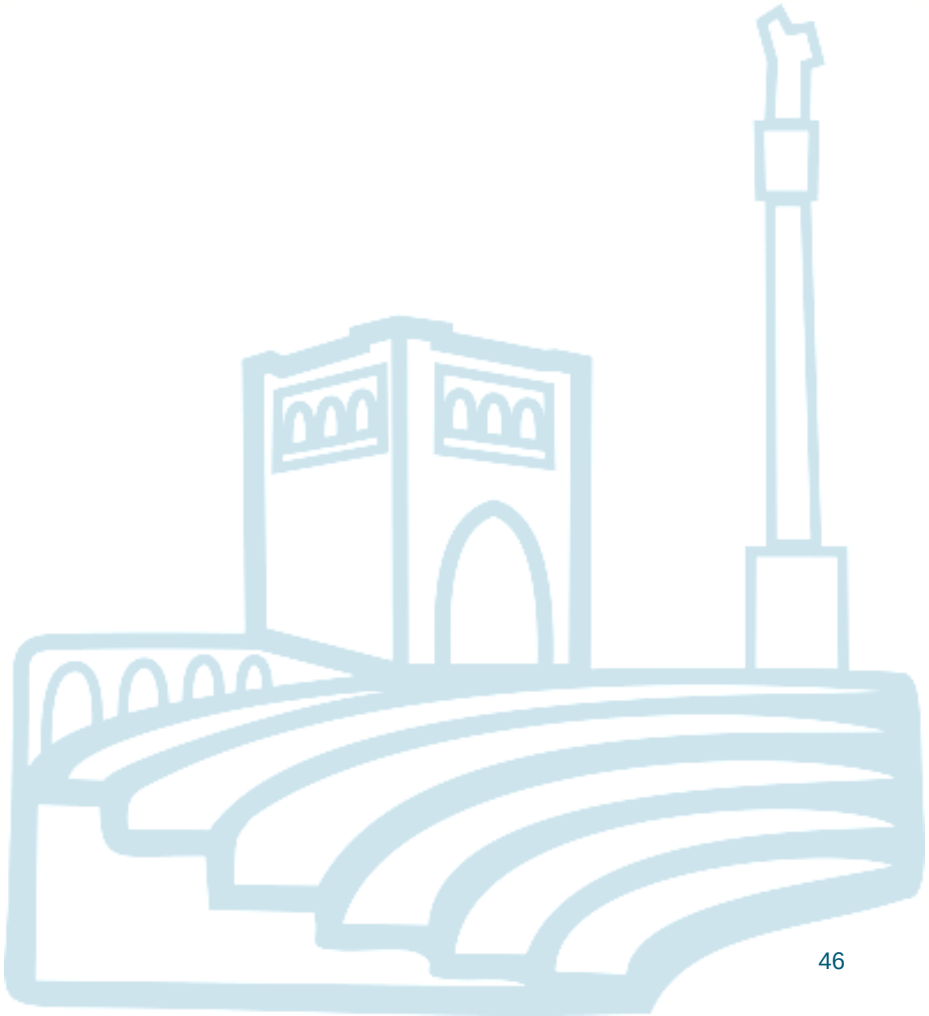
Delivery

Exploitation

Installation

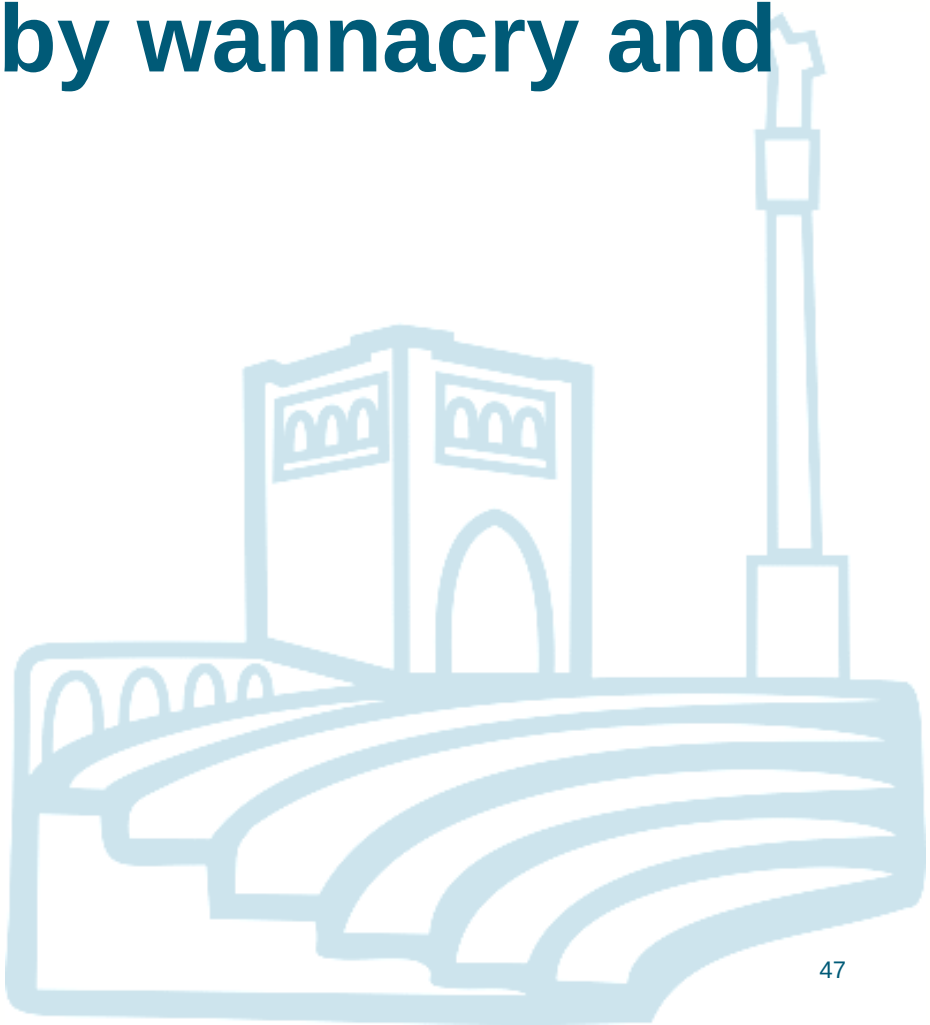
Command & Control

Actions on Objective



Eternablue is used by wannacry and non-petya ?

YES



Devices compromised during MIRAI

Videosurveillance camera

Stuxnet exploits vulnerabilities on … ?

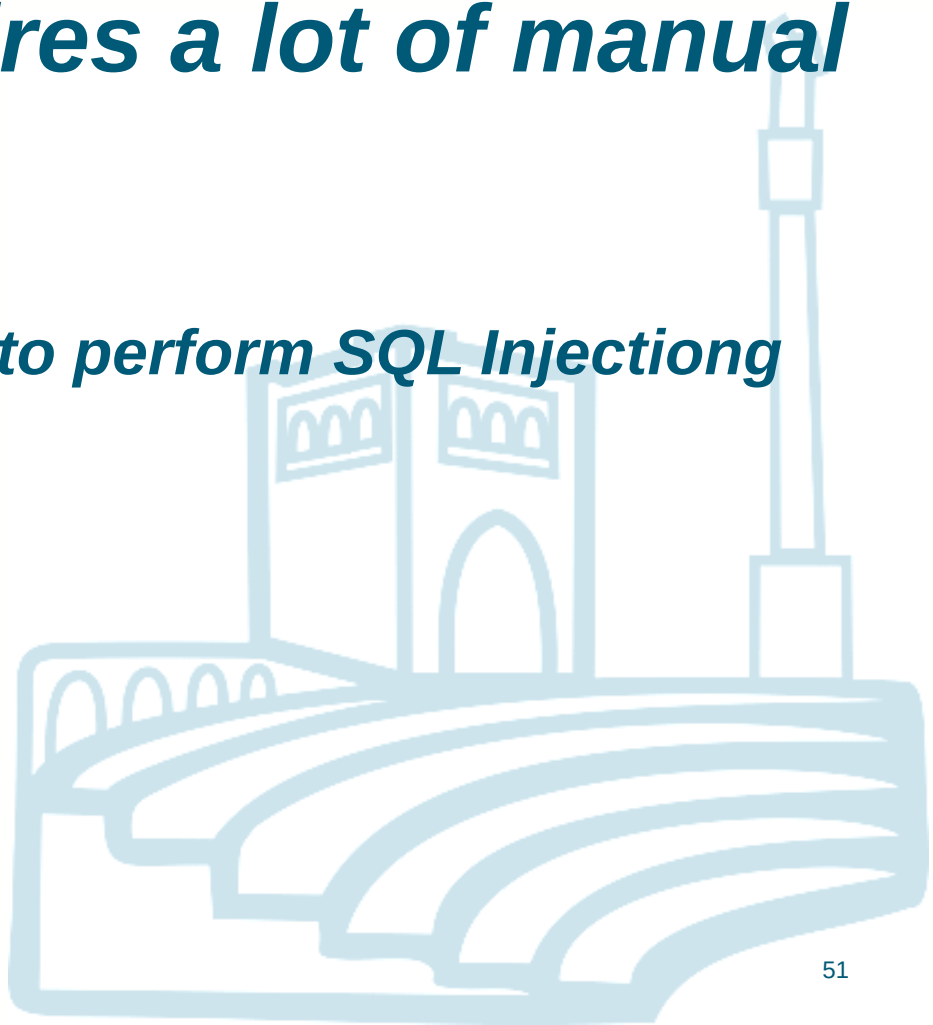
windows

Spoofing

Sender hides or changes something in the email to give the feeling that the email is arriving by someone legittimate

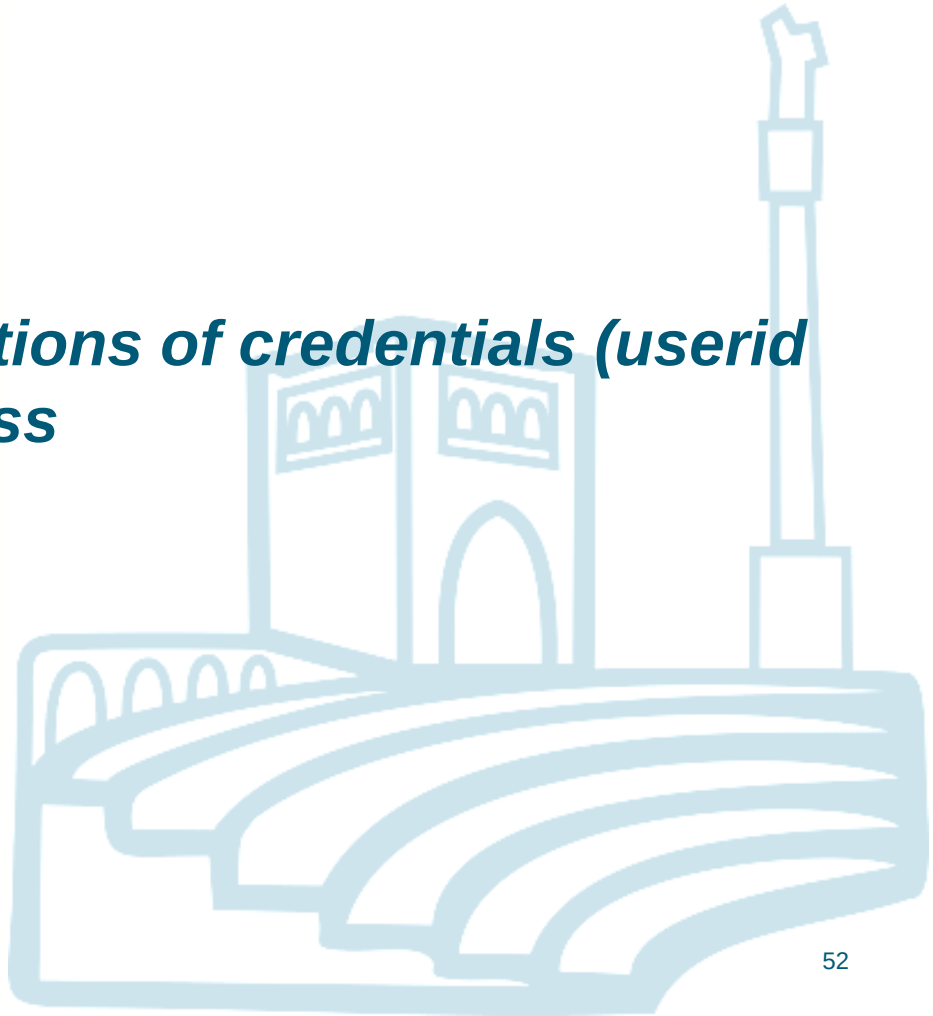
SQL Injection requires a lot of manual activitiesA

tool using AI can learn how to perform SQL Injectiong without none explaining



Brute Force

Trying all possible combinations of credentials (userid and password) to gain access



XSS

Remote Scripting is about programs running inside the browser to exchange information with the server

APT

An attack that is developed particularly for a specific customer

APT

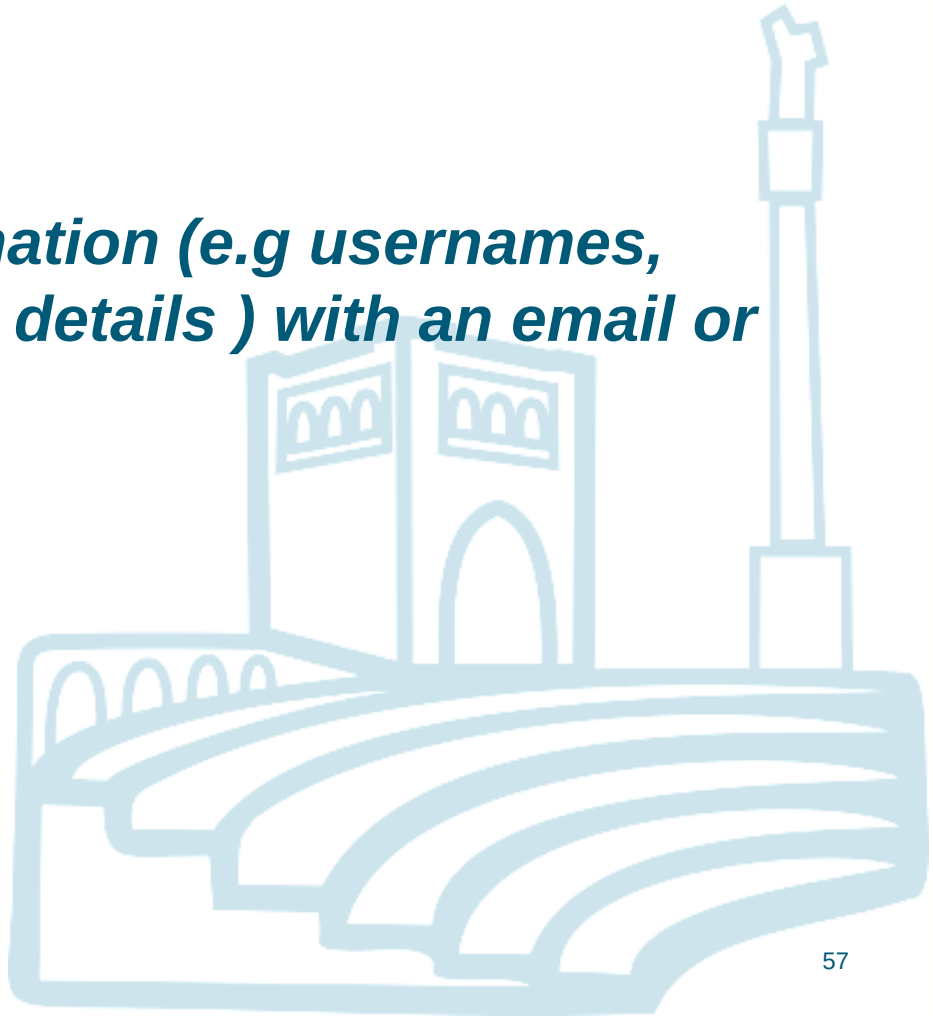
An attack that is developed particularly for a specific customer

Redirection Attack

The general idea is to redirect all the traffic to wrong site

Phishing

Obtaining sensitive information (e.g usernames, passwords ..... Credit card details) with an email or social network



DDoS

Deny of Service by creating a specific traffic that the service is not able to sustain

CVE

Common Vulnerabilities and Exposures

Security Controls

Identify, Protect, Detect, Respond, Restore

Access Management

Based on what you know, have and are

Thanks

Follow @domenicoraguseo
Follow @Exprivia_CY

www.exprivia.it