Problema da ciber-seguranca

* Software contem bugs
* Engenharia social é eficaz
* Encontrar e explorar vulnerabilidades é muito lucrativo

Porque comprometer a maquina de um utilizador

* Roubar passwords
* Ransomware (dinheiro)
* Como recursos (ex. minerar bitcoin)
* Usurpar endereço de rede e parecer utilizador normal (exercito de zombies)

Porque comprometer servidores

* Data breaches (números de cartão de credito de mts utilizadores, etc)
  + Consequências:
    - Pessoal (privacidade)
    - Credenciais (privacidade)
    - Alteração de comportamento
    - Instalação de software
    - etc
* Motivações politicas (hackers eletrical power grid da ucrania, etc)
* Para depois infetar maquinas dos utilizadores
  + Através de atualizacao de software
  + Através de servidores web

What is zerodium

Comprar exploits zero-day para depois vender a clientes

Definição de segurança

* Propriedade de um sistema comporta como esperado
* Protecao do computador de perda de informação, roubo ou dano de hardware, software ou dados eletronicos
* Sistema que permanece confiável ao encara o mal

Forma de pensar diferente

* Segurança é relativa
* Segurança muda consoante o contexto
* Segurança é defensiva (define-se pela negativa: tudo q não e bom n pode acontecer)

Atores

* Entidades q interveem no sistema
  + Pessoas, organizações, empresas, maquinas,…
  + Segurança define-se do ponto de vista destes atores
* Muitas vezes deposita-se confiança em alguns atores
  + Trusted third party, trusted agente
  + Sistema “seguro” se pressuposto de confiança se verificar
* Noutras, os atores são potenciais atacantes (externos/internos)

Adversario/atacante

* Importante conhecer o nosso adversário
  + Script-kiddies (curiosos mas incapazes)
  + Atacantes ocasionais para compreender o sistema
  + Pessoas com intenção de apenas causar danos
  + Grupos organizados e tecnicamente sofisticados
  + Competidores (espionagem industrial)
  + Países/estados/governos
* Importante pensar como um adversário:
  + Procurar sempre o elo mais fraco
  + Identificar pressupostos de confiança subjacentes à segurança
  + Olha para o sistema “outside the box”
    - Quem cria o sistema ta sempre preso ao q ele é suposto fzr