



# CYBER SECURITY



# MOTIVAÇÃO DO CRACKER

A motivação do hacker era financeira. Ele obteve acesso a informações confidenciais e, após criptografá-las, destruiu os dados originais. Em seguida, passou a exigir uma quantia em dinheiro para fornecer a chave de descriptografia e permitir o acesso novamente às informações. Ou seja, ele usou as informações como uma forma de extorsão, ameaçando prejudicar ainda mais a integridade dos dados caso suas exigências não fossem atendidas.

# VULNERABILIDADES(S)

## **Vulnerabilidade na Rede e Técnicas de Segurança**

Não uso de VPN (Rede Privada Virtual): A ausência de uma VPN pode expor os dados dos usuários a interceptações, tornando a comunicação vulnerável a ataques, especialmente em redes públicas.

## **Vulnerabilidade de Hardware**

Equipamentos mal configurados ou desatualizados, como servidores e dispositivos de rede, podem ser alvos de ataques físicos ou cibernéticos. O acesso não autorizado ao hardware pode comprometer a integridade dos dados armazenados.

## **Fragilidade nas Práticas de Segurança**

Ausência de políticas claras de segurança: Falta de treinamento e conscientização dos funcionários sobre práticas de segurança também é uma vulnerabilidade. Senhas fracas, falta de autenticação de dois fatores e o compartilhamento indevido de credenciais são exemplos de falhas humanas.

## **Fragilidade nas Práticas de Segurança**

Ausência de políticas claras de segurança: Falta de treinamento e conscientização dos funcionários sobre práticas de segurança também é uma vulnerabilidade. Senhas fracas, falta de autenticação de dois fatores e o compartilhamento indevido de credenciais são exemplos de falhas humanas.



# VULNERABILIDADES(S)

## Proteção de Dados Confidenciais

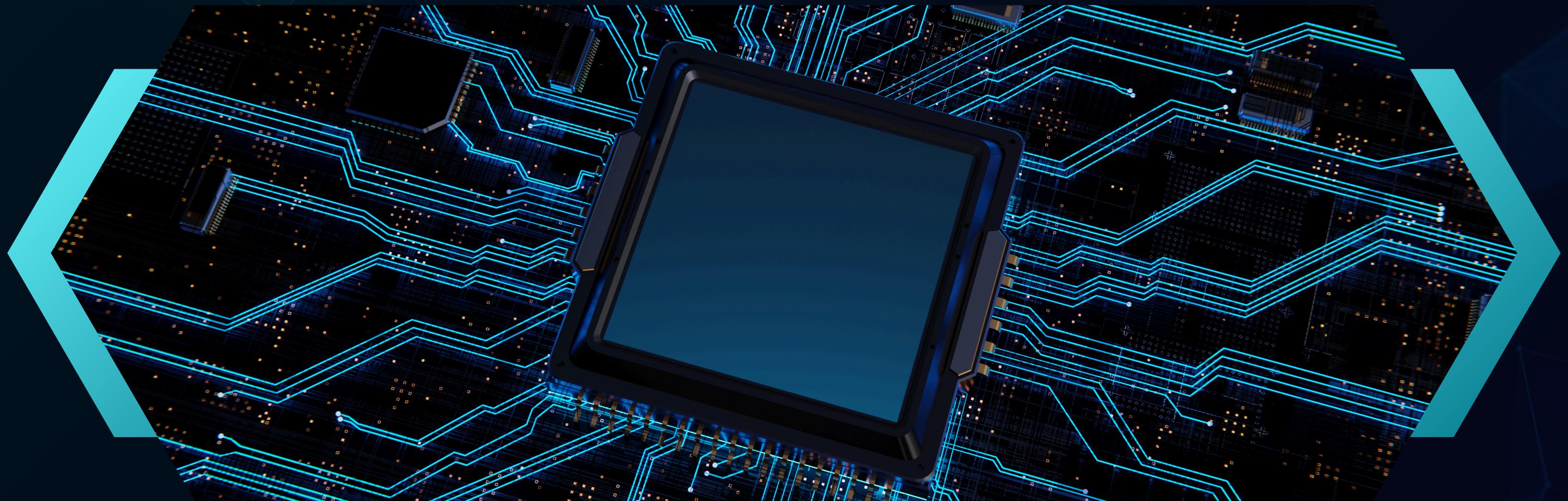
A proteção de dados sensíveis deve ser feita através de autenticação (garantindo que apenas usuários autorizados tenham acesso), autorização (controlando os direitos de acesso e ações dos usuários) e criptografia (garantindo que os dados estejam ilegíveis para quem não tem permissão).

## Rede Wi-Fi Não Monitorada:

Redes Wi-Fi abertas ou sem criptografia podem ser facilmente acessadas por atacantes. A falta de monitoramento dessa rede também dificulta a detecção de acessos não autorizados.

## Infraestrutura e Firewall Não Configurados

A ausência de uma configuração adequada de infraestrutura de segurança, como firewalls, pode permitir que ataques externos consigam acessar o sistema. Firewalls mal configurados ou desativados não bloqueiam tráfego malicioso e podem abrir brechas para ataques.





# TIPOS E TÉCNICAS DE ATAQUE UTILIZADOS

01

Spyware é um tipo de software malicioso projetado para monitorar e coletar informações sobre as atividades de um usuário sem o seu conhecimento. Ele pode registrar pressionamentos de teclas, capturar dados confidenciais, como senhas e informações bancárias, e até mesmo monitorar a navegação online.

02

A injeção de código é uma técnica em que um atacante insere código malicioso em uma aplicação ou sistema para executá-lo de forma não autorizada. Isso pode ocorrer em websites, aplicativos ou servidores, permitindo ao atacante manipular a execução do sistema, roubar dados ou até mesmo ganhar controle sobre o dispositivo.

05

# TIPOS E TÉCNICAS DE ATAQUE UTILIZADOS

03

Sniffing é uma técnica utilizada para interceptar pacotes de dados que trafegam por uma rede. Isso pode ser feito por atacantes para capturar informações sensíveis, como credenciais de login, dados bancários, e-mails ou outros dados privados. Normalmente, é feito em redes desprotegidas ou mal configuradas.

04

- IP Scanners: São ferramentas que varrem uma faixa de endereços IP para identificar os dispositivos e máquinas conectadas a uma rede. Ferramentas mais avançadas podem até obter o endereço MAC, que é um identificador único do dispositivo, facilitando a localização de máquinas na rede.
- Port Scanners: São ferramentas usadas para verificar as portas de comunicação abertas em sistemas e dispositivos. Comumente, os scanners de portas verificam portas TCP, que são usadas para estabelecer conexões de rede. Identificar portas abertas ajuda os atacantes a encontrar vulnerabilidades nos sistemas e facilitar o processo de invasão ou ataque.

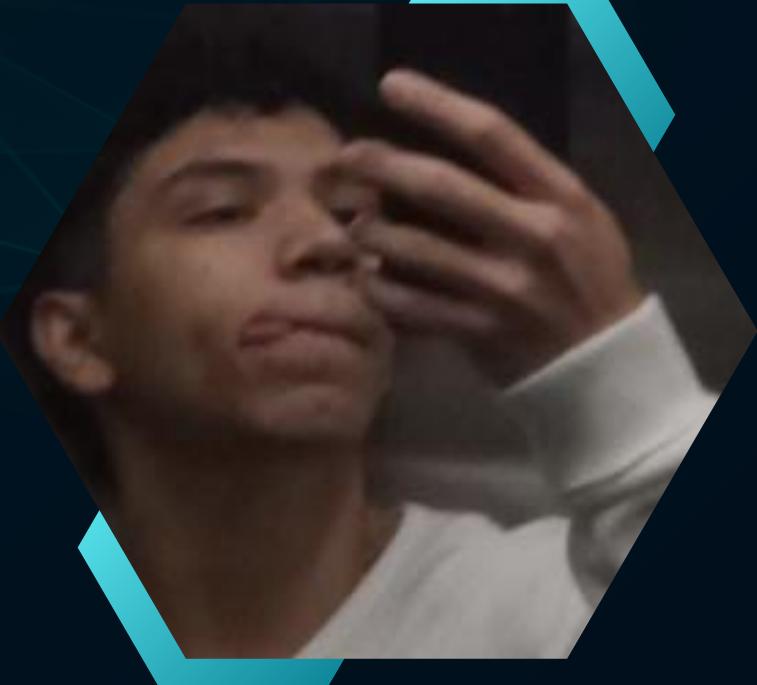


05

Um backdoor é um método malicioso utilizado por atacantes para obter acesso não autorizado a um sistema ou rede. Geralmente, ele é instalado por meio de vulnerabilidades ou como parte de um malware, permitindo que o atacante acesse o sistema posteriormente sem a necessidade de autenticação. Backdoors são especialmente perigosos, pois podem fornecer controle remoto do sistema comprometido.

06

# TEAM



**RAFAEL**

Rafael Alves, 20 anos, 5º semestre de engenharia de software e atualmente trabalhando.



**MAIDA**

Maida Chaparro, 20 anos, 5º semestre de engenharia de software e atualmente trabalhando.



**Bernardo**

Bernardo Oliveira, 19 anos, 3º semestre de engenharia de software e atualmente trabalhando.

# THANK YOU