

# ANATOMIA DE UM ATAQUE COMPLEXO

KATHLEEN LOHANNY DE SOUZA  
PEDRO HENRIQUE RIBEIRO BAPTISTA  
RICHARD ROSA GALINDO  
ISABELLE DE GODOY SANCHEZ  
PEDRO HENRIQUE FERREIRA DA ROCHA  
KAUÃ SANTANA OLIVEIRA



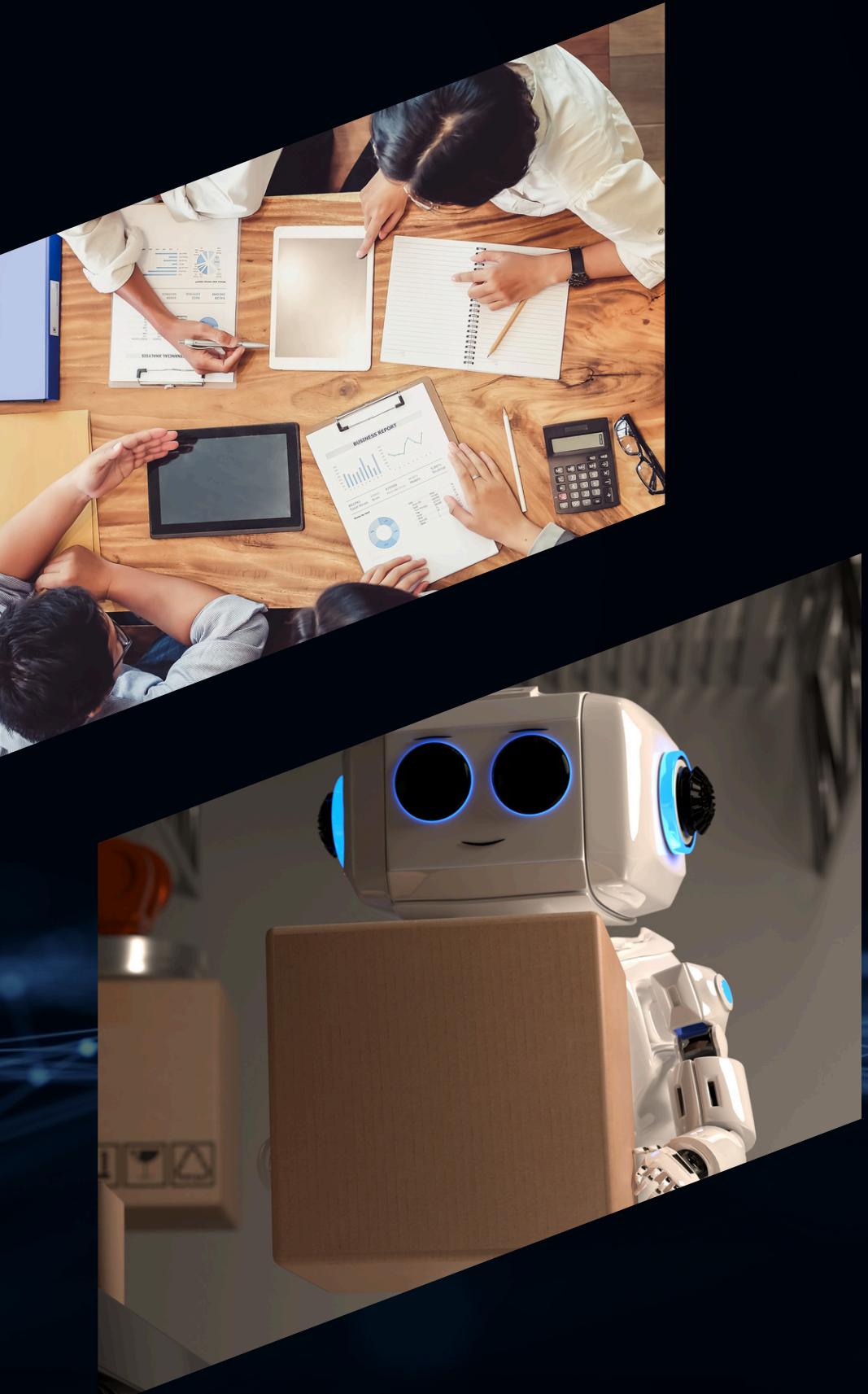
# VULNERABILIDADES



- **Falta de conscientização do usuário:** O phishing só funciona porque o usuário clicou em um link malicioso e forneceu credenciais;
- **Credenciais fracas ou mal protegidas:** Senhas não criptografadas ou armazenadas em planilhas do Excel tornam o acesso fácil.
- **Ausência de autenticação multifator:** Com apenas usuário e senha, o invasor consegue acesso completo;

# VULNERABILIDADES

- **Configurações inseguras de servidores:** Servidores de e-mail, arquivos ou banco de dados podem não ter restrições adequadas de acesso, permitindo que um invasor use credenciais válidas para se movimentar lateralmente;
- **Falta de monitoramento e alertas:** O invasor consegue copiar e deletar dados sem ser detectado, o que indica ausência de sistemas de detecção de intrusão (IDS/IPS) ou logs analisáveis.





# TIPOS E TÉCNICAS DE ATAQUES UTILIZADOS

## RECONHECIMENTO

Técnica: Varredura ativa para identificar sistemas e serviços disponíveis.

## ACESSO INICIAL

Técnica: Phishing (envio de e-mails falsos para roubar credenciais).  
Técnica: Uso de contas válidas com credenciais comprometidas.

## ESCALADA DE PRIVILÉGIOS

Técnica: Exploração de senhas armazenadas de forma insegura (planilhas não criptografadas).



# TIPOS E TÉCNICAS DE ATAQUES UTILIZADOS

## COLETA DE DADOS

Técnica: Extração de arquivos críticos do banco de dados.

## EXFILTRAÇÃO

Técnica: Transferência de dados pela rede para o invasor.

## IMPACTO

Técnica: Destruição de dados



# MOTIVAÇÃO DO CRACKER

- **Financeira**

Roubo de informações bancárias, dados de cartões de crédito ou dados corporativos valiosos;  
Venda de dados roubados no mercado negro;  
Ransomware: exige pagamento para devolver acesso aos dados.

- **Política ou estratégica**

Hacktivismo: ataque motivado por causas sociais ou políticas;  
Exposição de falhas de empresas ou governos para constrangê-los publicamente.

# MOTIVAÇÃO DO CRACKER



- **Satisfação pessoal / ego**

Desejo de provar habilidades técnicas, desafiar sistemas de segurança complexos;

“Destruição pelo desafio”: causar prejuízos ou caos apenas para demonstrar poder ou habilidade.

- **Competitiva**

Roubo de propriedade intelectual ou segredos comerciais para obter vantagem no mercado

# OBRIGADO

