

Professor: Robson Calvetti

Apresentação Atividade 2

São Paulo
2024

Integrantes do grupo:

Anabelly Rocha

Carolina Cruz

Maria Eduarda Moura

1. Vulnerabilidades do Site do Ataque

- O cracker encontra um site de automação de carros com falhas de segurança, sem medidas adequadas de proteção de dados.
- O site permite acesso às informações de engenheiros que trabalham com automação.
- Além disso, o site do boliche visitado pelos engenheiros é vulnerável a ataques, permitindo que o cracker injete código malicioso.

2. Técnicas Utilizadas

Reconhecimento: O cracker faz uma análise inicial para descobrir os engenheiros e suas rotinas, identificando que eles frequentam um boliche em dias específicos.

Exploração de Vulnerabilidades: Ele explora o site vulnerável do boliche, que possui falhas de segurança, como a ausência de proteção contra ataques de injeção de código.

Malware: O cracker insere um malware nas máquinas dos visitantes, aproveitando-se da falta de medidas de segurança no site. O malware é ativado quando os engenheiros acessam o site do boliche.

3. Motivação do Cracker

A principal motivação é obter informações dos engenheiros envolvidos com automação de carros. Ele visa roubar informações sensíveis através do controle remoto das máquinas comprometidas.

O ataque pode ter fins de espionagem corporativa, roubo de propriedade intelectual ou para obter vantagens financeiras ao vender as informações roubadas.

Conclusão

Este ataque exemplifica como a combinação de falhas em sistemas IoT e sites vulneráveis pode criar brechas para ataques cibernéticos que têm consequências graves, como o roubo de propriedade intelectual, espionagem corporativa e até prejuízos financeiros diretos. A defesa contra esses tipos de ataque requer uma abordagem proativa, como auditorias regulares de segurança, criptografia de ponta a ponta e educação dos funcionários sobre boas práticas de cibersegurança.