Universidade São Judas Tadeu - Mooca

Sistemas computacionais e Segurança

ANATOMIA DE UM ATAQUE COMPLEXO (IoT)

João Vitor Chioatto Serafim – 825133189

João Victor de Souza Moreira - 825135230

Professor: Robson Calvetti

São Paulo - SP
2025

Principais Vulnerabilidades

1. Site da pista de boliche
O site era antigo, com pouca manutenção e falhas de segurança, o que facilitou o acesso. O cracker utilizou uma injeção i-frame para inserir código malicioso. Assim, o notebook de um funcionário específico foi infectado ao acessar a página, tornando-se a porta de entrada para a rede corporativa da empresa.

2. Notebook do funcionário específico
O computador comprometido não possuía antivírus atualizado nem medidas de proteção eficazes. Isso permitiu que o malware fosse instalado e propagado sem ser detectado. A partir desse notebook, o cracker conseguiu explorar a rede interna e acessar sistemas críticos.

3. Dispositivo IoT (termostato)
O termostato conectado à rede corporativa apresentava firmware vulnerável e estava em uma rede simples, sem sub-redes ou segmentação. Isso permitiu que o cracker mantivesse acesso persistente à rede, mesmo após a empresa limpar o notebook infectado. O caso mostra como dispositivos IoT podem representar risco significativo quando não são isolados adequadamente.

4. Rede corporativa
A empresa não possuía segmentação de rede nem backup seguro. A ausência de um banco de dados externo ou de cópias em nuvem fez com que a exclusão de projetos e dados estratégicos causasse impacto direto e irreversível.

5. Fator humano
O funcionário que acessou o site vulnerável funcionou como vetor de ataque humano. Essa situação evidencia que a segurança da informação depende também de conscientização e treinamento de colaboradores.

6. Exposição de informações públicas
O cracker utilizou informações de redes sociais para localizar engenheiros e identificar hábitos, como frequentar a pista de boliche. Essa coleta de dados foi essencial para planejar o ataque e escolher o vetor mais eficaz.

Motivação do Cracker

1 - Financeira: venda dos projetos da empresa por 75 bitcoins.

2 - Estratégica: enfraquecer a empresa vítima e favorecer a concorrência no setor de veículos autônomos.

3 - Concorrência: indícios de que os dados foram entregues à empresa rival, que obteve vantagem na disputa.

4 - Reputação: ataques complexos podem aumentar o seu próprio prestígio e reputação cracker dentro da comunidade de hackers.

Tipos e Técnicas de Ataque Utilizados

1 - OSINT (Open-Source Intelligence): Coleta de informações públicas sobre engenheiros e seus hábitos, permitindo mapear potenciais vulnerabilidades humanas e escolher o melhor vetor de ataque.

2 - Injeção i-frame: exploração do site vulnerável da pista de boliche para inserir código malicioso que infecta os computadores de quem acessa a página.

3 - Malware em laptop de funcionário: instalação de software malicioso que funcionou como porta de entrada para a rede interna da empresa.

4 - Movimento lateral (Lateral Movement): técnicas utilizadas pelo cracker para se deslocar dentro da rede corporativa a partir do notebook infectado, explorando a ausência de segmentação.

5 - Exploração de IoT: uso do termostato vulnerável conectado à rede simples, permitindo persistência e acesso direto aos sistemas críticos da empresa.

6 - Exfiltração e exclusão de dados: retirada de projetos da empresa e destruição de arquivos importantes, aproveitando a ausência de backup seguro.

7 - Engenharia social indireta: aproveitamento de informações públicas sobre hábitos de funcionários para criar oportunidades de ataque, sem precisar de contato direto.