Anatomia de um Ataque Complexo

Vulnerabilidades

Website Antigo: A empresa vítima, Aupiticon, tinha funcionários que frequentavam um site de boliche antigo e, por consequência, mais vulnerável a ataques.

Rede "Plana": A rede da empresa não era segmentada, o que permitiu que o invasor, uma vez dentro do sistema, tivesse acesso irrestrito a todos os arquivos.

Dispositivo de IoT Não Verificado: Um termostato inteligente conectado à rede não foi inspecionado durante as varreduras de segurança, servindo como uma porta de entrada para o invasor.

Tipos e Técnicas de Ataque Utilizados

Watering Hole (Poço de Rega): O ataque foi iniciado comprometendo um site que era frequentemente visitado por um grupo específico de alvos — neste caso, os funcionários da Aupiticon que usavam o site da liga de boliche.

Injeção de I-frame: O invasor inseriu um código malicioso (i-frame) no site de boliche para infectar os computadores dos funcionários que o acessavam.

Engenharia Social: Antes do ataque, o invasor utilizou redes sociais para pesquisar e identificar os nomes dos engenheiros que trabalhavam na Aupiticon, tornando o ataque mais direcionado.

Acesso Através de Dispositivo IoT: Após a infecção inicial em um notebook, o invasor usou o termostato vulnerável que estava conectado à rede interna para ganhar acesso total aos sistemas da empresa.

Obtenção de Credenciais: As senhas e configurações padrão do termostato foram facilmente encontradas no site do fabricante, permitindo o acesso ao dispositivo.

Motivação do Cracker

Financeira: A principal motivação foi o lucro. O invasor, Brian Page, vendeu os projetos e plantas industriais roubados da Aupiticon em troca de 75 Bitcoins.
Ocultação de Rastros: Após concluir a venda dos dados, o invasor criptografou todos os discos rígidos e deletou os backups da empresa. A intenção era destruir as evidências e dificultar a recuperação da empresa, apagando seus rastros.