Nome: Beatriz Silva de Jesus

RA: 824219590

Anatomia de um ataque complexo

Vídeo analisado:
https://www.youtube.com/watch?v=TWX0m8bdwqQ

Vulnerabilidades Identificadas

1. Termostato Conectado à Rede: O termostato era um dispositivo IoT conectado à rede da empresa, o que proporcionou um ponto de entrada para os atacantes. Dispositivos IoT frequentemente têm menos segurança e podem ser uma porta para comprometer redes internas.
2. Malware no Site de Boliche: O malware foi projetado para infectar os laptops dos funcionários que visitassem o site de boliche. Esse site, sendo um ponto de encontro frequente para funcionários de empresas de tecnologia, foi explorado para atingir uma ampla gama de possíveis vítimas.

Tipos e Técnicas de Ataque Utilizados

1. Ataque via Malware em Site Comprometido: A técnica utilizada foi um ataque de drive-by download, onde o malware é instalado automaticamente no laptop do usuário quando ele visita o site comprometido. Esse tipo de ataque geralmente não requer interação adicional por parte do usuário além da visita ao site.
2. Exploração de Dispositivo IoT: O termostato foi explorado para obter acesso à rede interna da empresa. Dispositivos IoT muitas vezes têm segurança insuficiente e, quando conectados à rede principal, podem oferecer acesso a sistemas mais críticos e sensíveis.

Motivação do Cracker

A motivação principal foi o pagamento de 75 bitcoins, que equivale a uma quantia significativa de dinheiro. O fato de o pagamento ter sido solicitado por um contratante não identificado sugere que o ataque foi motivado por ganho financeiro. O objetivo final do ataque foi destruir dados críticos da empresa, incluindo backups. Isso demonstra um ataque de ransomware, onde os dados são criptografados ou excluídos para forçar a vítima a pagar um resgate para recuperá-los. A exclusão dos backups é uma estratégia para garantir que a empresa não possa restaurar os dados facilmente sem pagar o resgate. O ataque foi bem planejado e executado através de uma combinação de exploração de dispositivos vulneráveis e comprometimento de sites visitados pelos funcionários. A segurança de dispositivos IoT e a proteção contra malware são cruciais para proteger redes corporativas. Além disso, ter políticas robustas de backup e recuperação é essencial para mitigar o impacto de ataques de ransomware e garantir que a empresa possa se recuperar mesmo em caso de perda de dados.