Paulo Henrique Luiz do Monte

RA: 82325475

Atividade: ”Anatomia de um ataque complexo”

1. Vulnerabilidades Identificadas

As principais vulnerabilidades exploradas pelo cracker no ataque foram:

- **Vulnerabilidade Humana e de Processos:** O ataque se inicia com a coleta de informações em redes sociais sobre os funcionários da empresa-alvo (Aupticon). O cracker descobre que os engenheiros participam de uma liga de boliche, identificando um alvo e seu comportamento fora da empresa.
- **Segurança de Terceiros (Cadeia de Suprimentos):** A primeira infiltração não foi na empresa, mas sim no site do boliche frequentado pelo funcionário, que era um site pequeno e com segurança fraca.
- **Software Desatualizado (Falta de *Patching*):** O cracker utiliza um *exploit* antigo em um *Iframe* no site do boliche, explorando uma vulnerabilidade conhecida e não corrigida para infectar o laptop do engenheiro.
- **Vulnerabilidade de Dispositivos IoT (Internet das Coisas):** O ponto de entrada na rede interna da empresa foi um termostato inteligente. Este dispositivo estava rodando software desatualizado e, crucialmente, utilizava senhas e configurações padrão do fabricante, que estavam publicamente disponíveis online.

2. Tipos e Técnicas de Ataque Utilizados

O ataque foi complexo e multifacetado, combinando diversas técnicas em sequência:

1. **Reconhecimento e Engenharia Social:** O cracker inicia pesquisando sobre os funcionários em redes sociais para encontrar um "elo fraco" e entender seus hábitos, o que é uma forma de engenharia social.
2. **Ataque *Watering Hole* (Poço de Água):** Em vez de atacar a empresa diretamente, o cracker compromete um site que ele sabe que seu alvo irá visitar (o site do boliche).
3. ***Iframe Injection* (Injeção de Iframe):** No site do boliche, ele injeta um *Iframe* malicioso que contém um *exploit*. Quando o engenheiro visita a página, seu computador é infectado sem que ele perceba.

4. **Movimentação Lateral:** Uma vez que o laptop do engenheiro se conecta à rede interna da Aupticon, o cracker utiliza essa conexão para "pular" para dentro da rede corporativa.
5. **Escalada de Privilégios via IoT:** O cracker identifica o termostato na rede, acessa-o usando as senhas padrão do fabricante e o utiliza como pivô para ganhar acesso a outras partes da rede.
6. **Exfiltração de Dados:** Com acesso total, ele navega pelos servidores e rouba informações críticas, como arquivos do RH, documentos jurídicos e projetos de pesquisa e desenvolvimento (P&D).
7. **Ataque de Ransomware / Destruição de Dados:** Após roubar os dados, o cracker executa a fase final: criptografa todos os arquivos nas unidades da empresa e apaga os backups, paralisando completamente a Aupticon.

3. Motivação do Cracker

A motivação principal do cracker é **financeira**. Ele foi contratado para realizar o ataque e, como pagamento, recebeu **75 Bitcoins**.

Além do ganho financeiro, o cracker demonstra um elemento de satisfação pessoal e desafio, mencionando que fez aquilo "um pouco por brincadeira", o que revela uma motivação secundária ligada ao poder e à emoção de realizar um ataque bem-sucedido.