GRUPO: Acácio, Daniel Silva, Matheus Bolato e Munir.

CONTEXTO:

Durante as aulas de Sistemas computacionais e segurança, foi apresentada uma atividade de análise com o intuito de identificar, em uma produção áudio visual, as vulnerabilidades, tipos de técnicas utilizados pelo cracker e suas motivações.

Link do vídeo: https://video-br.cisco.com/detail/video/5620318141001

RESUMO DO VÍDEO:

A anatomia de um ataque IOT

O FBI prendeu um homem em San Francisco por invadir e atacar ciberneticamente um centro de pesquisa chamado Aupticon, que estava trabalhando no desenvolvimento de câmeras de rastreamento óptico para carros sem motoristas.

O criminoso começou pesquisando nas redes sociais pelos nomes de vários dos engenheiros que trabalhavam lá e durante a busca se deparou com uma liga de boliche onde várias empresas de tecnologia se reuniam às quartas-feiras. O estabelecimento era bem antigo e possuía um site bem ultrapassado, que continha os nomes das empresas e dos jogadores participantes.

O cracker invadiu o site do boliche com um ataque iFrame injection, infectando todos que entravam nele. Dessa maneira, após uma semana, o invasor teve acesso à rede da empresa por intermédio de um computador de um funcionário que foi infectado por esse malware.

Assim que se infiltrou na Aupticon, direcionou seu ataque para um termostato conectado à rede, explorando-o como um dispositivo vulnerável para manter acesso contínuo e expandir o alcance do ataque, pois não recebia vistoria da segurança.

Explorando a rede da empresa, percebeu que ela era muito simples e quase não tinha proteção. Ele encontrou vários arquivos do RH, documentos jurídicos, P&D e se deu conta de que poderia ganhar muito dinheiro com a venda dessas informações.

Após comercializar diversos registros da Aupticon para uma empresa rival por 75 bitcoins (110.485 dólares na cotação atual 09/25), ele destruiu tudo, limpou tudo que encontrou, criptografou as unidades e excluiu os backups na tentativa de encobrir qualquer pista.

MOTIVAÇÃO:

- O ataque foi movido por ganho financeiro, com recompensa paga pela empresa rival.

VULNERABILIDADES:

Identificação fácil de quem trabalha na Aupticon pelas redes sociais:

- A ausência da conscientização digital permitiu que perfis de funcionários fossem facilmente identificados em redes sociais, expondo informações que podem ser exploradas em ataques.

O mesmo laptop que o funcionário usa em casa é o mesmo que ele usa na empresa:

- O uso do mesmo dispositivo em ambientes pessoais e corporativos representa uma falha do profissional, aumentando o risco de "contaminação" e comprometimento da rede corporativa por meio de vulnerabilidades exploradas em uso pessoais.

O site do boliche é ultrapassado e possui as informações dos funcionários e empresas de tecnologia:

- A utilização de um site desatualizado e a exposição de dados de colaboradores e usuários, representa um ponto crítico de vazamento de informações sensíveis.

A rede da Aupticon é muito simples, praticamente sem nenhuma segurança

- A infraestrutura de rede da Aupticon não tem camadas de proteção adequadas, apresentando-se como um ambiente sem monitoramento ou mecanismos de defesa, o que amplia significativamente a possibilidade de ataque.

TÉCNICAS DE ATAQUE UTILIZADAS:

Comprometimento inicial:

- O cracker invadiu o site da liga de boliche e fez um ataque iFrame Injection. Esse ataque consiste na inserção de um elemento HTML iframe malicioso em um site sem permissão, podendo permitir ataques como phishing, instalação de malware e roubo de dados.

Infecção de dispositivo:

- Um funcionário da Aupticon acessou o site comprometido e teve seu laptop infectado.

Acesso à rede corporativa:

- Como o funcionário usava o mesmo laptop em casa e na empresa, o invasor obteve acesso inicial à rede da Aupticon.

Exploração de IoT:

- O cracker comprometeu o termostato conectado à rede, ainda com senha padrão de fábrica, usando-o como ponto de persistência e movimentação lateral.

Exfiltração de dados:

- Documentos sensíveis foram copiados e vendidos para uma empresa rival.

Acobertamento do crime:

- A fim de não ser encontrado, destruiu todos arquivos que conseguiu encontrar, criptografou as unidades e excluiu os backups da Aupticon.