Anatomia de um Ataque IoT

Cenário

A empresa fictícia **Opticon** está desenvolvendo um **carro autônomo**. O vídeo detalha como um atacante, chamado **Brian**, consegue comprometer a infraestrutura da empresa, explorando vulnerabilidades tanto em dispositivos IoT quanto na própria rede corporativa.

Etapas do Ataque

1. Reconhecimento / Seleção de alvo

- Brian pesquisou redes sociais para identificar engenheiros da Opticon.
- Descobriu que esses engenheiros participavam de uma liga de boliche que usava um site antigo para registrar partidas e nomes de empresas.

2. Comprometimento do ponto de entrada externo

- O atacante injetou malware via *iframe injection* no website da boliche.
- Qualquer visitante do site, incluindo engenheiros da Opticon, teve seu laptop infectado.

3. Entrada na rede corporativa

- O laptop infectado foi conectado à rede da Opticon.
- A rede corporativa era **plana** (sem segmentação), permitindo ao atacante acesso a diversas áreas críticas, incluindo arquivos de RH, jurídico e P&D.

4. Exploração de dispositivos IoT e credenciais fracas

- Brian percebeu que o termostato conectado à rede corporativa estava inseguro.
- Obteve rapidamente as credenciais padrão do fabricante, sem dificuldade.

5. Movimentação lateral e acesso a dados críticos

- Utilizando a rede plana e o dispositivo IoT, o atacante moveu-se lateralmente e encontrou **blueprints de P&D** valiosos da empresa.

6. Destruição, criptografia e extorsão

- Brian criptografou discos, deletou backups e dificultou a recuperação da empresa.
- Recebeu **75 bitcoins** como pagamento pelo ataque.

7. Impactos para a empresa

- A Opticon perdeu vantagem competitiva no mercado.
- As ações da empresa despencaram e a recuperação da rede exigiu restauração completa a partir de backups, que foram comprometidos.

Vulnerabilidades Exploradas

- Dispositivos IoT com **credenciais padrão**.
- **Rede plana** sem segmentação de sub-redes.

- **Laptop infectado** conectado diretamente à rede corporativa.
- **Backups acessíveis** e não protegidos.
- Falta de **monitoramento e escaneamento** de dispositivos IoT.

Técnicas de Ataque Utilizadas

- **Iframe injection** em website público.
- **Malware persistente** no laptop do engenheiro.
- Uso de **credenciais padrão** de IoT.
- **Movimentação lateral** dentro da rede corporativa.
- **Ransomware**: criptografia de discos e deleção de backups.
- **Encobrimento de rastros** para dificultar investigação.

Motivação do Atacante

- **Financeira**: pagamento em bitcoins.
- **Sabotagem / vantagem competitiva**: ao prejudicar a Opticon, concorrentes se beneficiaram.
- O ataque foi planejado e profissional, demonstrando que não se tratava de uma ação “por diversão”.

Lições Aprendidas

- Dispositivos IoT devem ser **protegidos e segmentados** da rede corporativa.
- **Credenciais padrão devem ser alteradas** imediatamente.
- Redes corporativas precisam de **segmentação e monitoramento** adequados.
- **Backups** devem ser isolados e protegidos.
- A superfície de ataque inclui até dispositivos simples, como termostatos.
- Preparação e conscientização dos usuários são essenciais para evitar que endpoints comprometam a rede.

Gustavo Jaccon Franquini
RA: 825150548