UNIVERSIDADE SÃO JUDAS TADEU

GUILHERME SILVA MORENO RA: 825137659

LUCAS PERES SIMÕES RA: 825154655

MIKE BRIAN MAGATI DOS SANTOS RA: 825130703

PEDRO HENRIQUE GUIMARÃES RESTANI RA: 825155169

RICARDO SIQUEIRA LOIOLA RA: 825154725

ANATOMIA DE UM ATAQUE DE IoT

Vulnerabilidades, Táticas e Motivos

São Paulo

2025

UNIVERSIDADE SÃO JUDAS TADEU

GUILHERME SILVA MORENO RA: 825137659

LUCAS PERES SIMÕES RA: 825154655

MIKE BRIAN MAGATI DOS SANTOS RA: 825130703

PEDRO HENRIQUE GUIMARÃES RESTANI RA: 825155169

RICARDO SIQUEIRA LOIOLA RA: 825154725

ANATOMIA DE UM ATAQUE DE IoT

Vulnerabilidades, Táticas e Motivos

Pesquisa destinada para obtenção de nota na UC Sistemas Computacionais e Segurança em Análise e Desenvolvimento de Sistemas apresentado à Universidade São Judas Tadeu – USJT

Orientador: Prof. Robson Calvetti

São Paulo

2025

Introdução

Pesquisa sobre o video “Anatomia de um ataque de IoT”, motivos, vulnerabilidades e táticas de um Cracker. Cracker que foi responsável por invadir a empresa de veículos autônomos “Aupticon” e vazou informações confidenciais, levando a empresa à danos severos e perda de mercado.

Vulnerabilidades

As vulnerabilidades apresentadas mostram como é fácil um Hacker mal intencioando (Cracker) conseguir invadir empresas e causar danos que muitas vezes podem ser irreversíveis. As vulnerabilidades analisadas são:

- **Site de boliche desatualizado e com brechas de segurança.**

O Boliche que um dos funcionários frequentava e tinha seus dados cadastrados em seu sistema era muito fraco e tinha diversas brechas de segurança, muito por conta de ser um sistema antigo. Com essas falhas, o Cracker conseguiu facilmente inserir um malware no site, assim fazendo com que qualquer um que acessasse o site, teria sua máquina infectada com o malware, uma dessas vítimias foi um funcionário da empresa, que quando levou seu laptop para empresa e acessou a rede da mesma, infectou a empresa toda.

- **Termostato.**

Mesmo com o descobrimento do vírus dentro da empresa e todas as precauções para eliminá-lo, e pensarem que haviam verificado a rede inteira, ainda havia um Termostato ligado à rede, ainda dentro do firewall. O Termostato tem todas suas configurações e senhas online, de fácil acesso para qualquer um, basta acessar o site do fabricante.

- **Rede Corporativa Vulnerável.**

Após ainda estar dentro do sistema da empresa por conta do Termostato, o Cracker tinha acesso a tudo, arquivos do RH, documentos jurídicos, P&D, tudo por conta de um sistema frágil de segurança da própria empresa.

Tipos e Técnicas de Ataque

- **Engenharia Social**

O Cracker, através de simples pesquisas na internet, conseguiu dados dos funcionários que trabalhavam na Aupticon. Ao obter a informação de um deles, percebeu que o funcionário frequentava uma pista de boliche, acessando o site dessa pista, notou o quanto o site era vulnerável e se aproveitou disso, injetando um malware no site e infectando qualquer um que o acessasse.

- **Injeção do Malware**

Por conta do site ser datado e ter muitas falhas de segurança, o Cracker conseguiu facilmente injetar um malware e infectar o funcionário que frequentava o site, assim que o funcionário levou seu laptop infectado à empresa e acessou sua rede, todo o sistema estava comprometido.

Motivação

No vídeo, o Cracker fala que o motivo do ataque foi a quantia de 75 bitcoins (R$ 45.057.125,42 na cota atual, 09/2025) , porém, é de fácil compreensão que a responsável por pagar essa quantia foi a empresa concorrente, pois ao fim do vídeo é perceptível o aumento nas vendas e no mercado da Qcar, empresa concorrente.

Maneiras de Evitar

- **Treinamento e Conscientização.**

Empresas deveriam treinar seus funcionários sobre golpes comuns, limitar o nivel de informações públicas de seus funcionários e aumentar as políticas de segurança de empresa, tais como: Não trazer componentes eletrônicos de casa, apenas os fornecidos pela empresa e orientar a não injetar pendrives desconhecidos nas máquinas da empresa.

- **Aumentar a segurança da rede.**

Um dos maiores fatores para o Cracker permanecer e ter acesso a informações confidenciais, foi a fraqueza na segurança da empresa. Deveriam ser implementados sub-redes para separar departamentos, melhorar o controle de acesso com autenticação multifator e o maior fator para melhorar a segurança da empresa, seria o treinamento do usuário, visto que ele é a maior brecha do sistema, foi por conta dele que a empresa teve todo o prejuízo.

Conclusão

Em suma, a Aupticon (Empresa Vítima) teve prejuízos irreversíveis e a Qcar (Empresa Responsável por Pagar o Cracker) teve vantagem no mercado. Toda a situação aconteceu por conta de uma simples técnica de engenharia social, junto a um sistema de segurança fraco. Novas normas de segurança e treinamento de usuário deveriam ser implementadas anteriormente para evitar o ocorrido.

Vídeo Analisado

https://video-br.cisco.com/detail/video/5620318141001