- **Kauê Soares Dos Santos - 824117267**
- **Leonardo Macedo Camargo - 82422817**
- **Luiz Washington de Jesus Muraro - 824148694**
- **Lucas Felipe Monteiro Suarez - 824138683**
- **George Geronimo Menezes Ferreira - 824148488**

Análise do Vídeo ”Anatomia de um ataque complexo”

Vulnerabilidades: Os funcionários que utilizam dos próprios aparelhos para se conectar a redes fora da empresa se apresentam como um risco para vulnerabilidade da empresa, falta de redes segmentadas por setores ou outros critérios pode facilitar que invasores acessem áreas da empresa que deveriam ser acessadas apenas por funcionários autorizados, pouca preocupação na verificação de dispositivos secundários (como no vídeo que a backdoor do cracker foi o termostato da empresa que não foi verificado, sendo assim um meio para retornar), senhas padrões de dispositivos de fábricas sendo facilmente descobertas por uma simples pesquisa na internet (senhas fáceis também facilitam a entrada do invasor).

Possíveis vulnerabilidades do sistema

Falhas de controle de origem: A política de mesma origem (Same-Origin Policy) é uma medida de segurança dos navegadores que impede que scripts de um domínio acessem dados de outro. No entanto, se essa política for burlada ou mal configurada, um iframe malicioso pode ser usado para acessar ou manipular dados de uma página da web legítima.

Inserção de conteúdo externo inseguro: Algumas aplicações web permitem que administradores ou usuários incorporem conteúdo externo (como vídeos ou outros recursos de sites terceiros) sem verificarem a origem ou o conteúdo desses recursos. Isso pode ser explorado se o conteúdo externo for controlado ou comprometido por um atacante.

Permissões de conteúdo flexíveis: Um site que permite a inclusão de HTML em comentários, perfis ou outras seções dinâmicas pode, inadvertidamente, abrir espaço para a injeção de iframes maliciosos.

Tipos e técnicas de ataques utilizados

Ataque de injeção I-frame: Um cracker injeta um código `<iframe>` malicioso em um site vulnerável, muitas vezes aproveitando falhas como XSS (Cross-Site Scripting) ou fraquezas em plugins desatualizados (como exemplificado no vídeo,

onde o cracker usa um site de boliche para roubar as informações dos funcionários que acessam o site).

Motivação do Cracker

A motivação do cracker no começo foi a curiosidade, mas logo depois de ver os arquivos da empresa ele percebeu que poderia vender aquelas informações para a concorrência por 75 bitcoins.