NOMES:

ANDREY FERREIRA PICHUTI / RA: 82414002

MOSHE ACHKIY SILVERIO MANDUJANO / RA: 824115318

JOÃO GABRIEL SILVA BARBARA DA CONCEIÇÃO / RA: 82415176

NICOLAS TRINDADE MARCIANO / RA: 824135758

ANATOMIA DE UM ATAQUE COMPLEXO

O vídeo apresenta um ataque que ocorreu contra a Aupticon, uma empresa que estava em uma disputa com outras para a fabricação do primeiro carro autônomo. Com o ataque, a empresa perdeu praticamente todos os arquivos relacionados ao projeto, inclusive os backups, e o prejuízo foi imensurável, além das ações da empresa terem caído logo após a Qcar lançar o QX Sedan, o primeiro carro com direção autônoma do mundo.

VULNERABILIDADES:

O vídeo apresenta duas principais vulnerabilidades, as quais citarei a seguir:

1° Site de boliche: Brian, o hacker responsável pelo ataque, tinha que, de algum jeito, conseguir entrar na rede da empresa. Ele foi no site da Aupticon, o qual possuía o nome de vários funcionários e, ao pesquisar alguns nomes no navegador, ele descobre que existe uma espécie de liga de boliche que ocorre entre algumas empresas de tecnologia, todas às quartas-feiras. O site da liga é antigo, possui o nome das empresas, jogadores e todas as informações sobre a liga, e justamente por ser um site desenvolvido antigamente, sem políticas de segurança atualizadas, o hacker conseguiu invadir facilmente e implantar um malware no site.

2° Termostato: O hacker, após conseguir acesso à rede, obviamente foi silenciado pelos funcionários da empresa pelo sistema de segurança, porém o que a Aupticon não esperava, é que o termostato da empresa estava conectado à rede, e foi por ele que o hacker conseguiu fazer todos os processos que precisava para fazer o seu ataque.

TIPOS E TÉCNICAS DE ATAQUE UTILIZADOS:

O principal tipo de ataque utilizado pelo hacker foi um ataque de injeção i-frame. Como citado nas vulnerabilidades, o site da liga de boliche era antiquado, não tinha um sistema de segurança bom, o que possibilitou o hacker a utilização dessa técnica.

Injeção i-frame é um tipo de ataque em que, todo mundo que acessa o site afetado, é infectado por um malware manipulado pelo hacker. Detalhando ainda mais, o hacker insere um iframe, que é uma página HTML embutida em outra página, porém com o conteúdo malicioso. Esse tipo de ataque pode ser utilizado para vários fins, como Phishing, Clickjacking ou entrega de malware, como foi o caso.

MOTIVAÇÃO DO CRACKER:

O que mais motivou o cracker a realizar o ataque à Aupticon foi com certeza o pagamento. No final do vídeo, Brian revela que ganharia 75 bitcoins se conseguisse apagar todos os arquivos da empresa. Isso hoje equivale à U$ 4522612,50.