

LUCAS BENITE
DE ALCANTARA
RA: 824157974

O cracker conseguiu em redes sociais, os nomes de vários engenheiros que trabalhavam no centro de pesquisa, em um projeto de câmeras de rastreamento óptico para carros sem motoristas e durante a pesquisa, achou uma liga de boliche, onde várias empresas de tecnologia jogavam. O A pista era antiga, o site antigo, com os nomes das empresas e jogadores. O ataque utilizado contra o site foi uma injeção de i-frame, que é uma técnica de ciberataque que envolve a inserção de um iframe em um site sem a permissão do proprietário. Um iframe é um elemento HTML que permite incorporar conteúdo de outro site numa página da web e ataca todos que o visitam. Então, um funcionário da empresa alvo, que visitou o site da liga de boliche, teve o malware do cracker instalado no seu notebook. No dia seguinte, o funcionário vai à empresa e conecta seu notebook à rede, o que coloca o cracker dentro dela. A empresa descobriu, limpou o laptop, mas não verificou toda a rede. O termostato que ficava conectado à rede, dentro do firewall foi usado para que o cracker obtivesse toda a configuração padrão e senhas pelo site do fabricante desse termostato, isso o tornou uma vulnerabilidade da rede. O cracker acessa e descobre que a rede é simples, sem sub-rede nem nada. Teve acesso aos arquivos de RH, documentos jurídicos e aos projetos. Quando ele acessou os projetos, percebeu que poderia ganhar dinheiro com os arquivos deles, então, enviou os projetos para si mesmo e os destruiu, criptografou e excluiu backups, tudo para encobrir pistas. O cracker foi pago para isso. Um tempo depois, uma outra empresa apresentou seu primeiro carro com direção autônoma, o primeiro do mundo.