

Anatomia de um ataque complexo

Informações retiradas com base no vídeo: <https://video-br.cisco.com/detail/video/5620318141001>

Vulnerabilidades: talvez não ter verificado completamente a rede e todos os dispositivos que poderia ser acessado remotamente pelo cracker.

Tipo e técnicas de ataque utilizados: o cracker utilizou o ataque de injeção de I-Frame, injetou esse sistema no site que desejava atacar, a partir desse momento todos que acessam o site fica exposto tendo o malware do cracker inserido no seu dispositivo facilitando o acesso dele remotamente.

Motivação: Financeira, a partir do momento que ele teve acesso a todos os documentos e arquivos da empresa aupticon, ele percebeu que poderia ganhar algum dinheiro com aquilo, e foi o que ele fez vendendo todas essas informações por 75 bitcoins.