ATIVIDADE 02

Docente: Robson Calvetti
UC: Sistemas Computacionais e Segurança – SCS

Marinna Pereira Carneiro da Silva
RA: 824142121
Análise e Desenvolvimento de Sistemas - ADS

Att, Marinna

ATIVIDADE 02 - Para a próxima aula: Pesquisa e apresentação;

Regras:

- Em grupo, assistir, identificar no vídeo e responder:

Vulnerabilidades(s): Falta de verificação de segurança e práticas inadequadas para proteger dados confidenciais em redes conectadas.

Tipos e técnicas de ataque utilizados: Injeção de iFrame (Code Injection) e instalação de spyware para coleta de dados.

Motivação do cracker: Obter lucro financeiro através da venda de informações obtidas ilegalmente.

- Tema: ”Anatomia de um ataque complexo”

Link - https://www.youtube.com/watch?v=TWX0m8bdwqQ

Att, Marinna

ATIVIDADE 02

As vulnerabilidades encontradas no vídeo podem ser facilmente identificadas onde o Cracker denominado “Brian” debocha de como foi intencional o acesso de invadir o site de uma pista de boliche, onde não possuía uma grande segurança e conseguiu ter uma chance perfeita de ter acesso aos dados dos engenheiros do Centro de Pesquisa “Auption” afins de buscar lucro.

Identificando no vídeo e podemos notar que o Cracker conseguiu entrar no site da pista de boliche com uma das técnicas de ataque denominada injeção de iframe a famosa Code Injection onde envolve a inserção de um iframe (elemento HTML) em um site sem a permissão do proprietário onde permite incorporar conteúdo de outro site numa página da web e pela essa injeção o Cracker conseguiu pela falta de verificação, ou seja, a falta nas práticas de segurança na hora de proteger dados confidenciais através de uma autenticação do termostato, ele conseguiu acessar a rede da pista de boliche e coletar os dados instalando o seu malware no dispositivo infectado utilizando o spinware onde em um software oculto e autônomo, ou seja, o Cracker recolhe as informações dos usuários desejados.

O cracker fala em seu depoimento de como foi “fácil” entrar pela essa técnica, em menos de uma semana ou um dia, quando o proprietário leva o computador para a pista de boliche e conecta a rede ele consegue ter acesso a vários dados de usuários, ou seja, os dados dos engenheiros que comentamos anteriormente. Onde possuía arquivos de RH como dados pessoais de contas bancárias, documentos jurídicos de processos, senhas dos usuários, configuração padrão e projetos da Auption de carros que nem sequer tinham sido produzidos pelos engenheiros em 10 segundos somente ele conseguiu ter todos esses acessos.

A sua motivação como Cracker sempre foi obter lucro, como o mesmo descreve recebeu uma quantia de 72 bitcoins que hoje em dia custam em média R$ 23.555.347,00 contando que o bitcoin está valendo em real R$327.157,00. O vídeo conclui mostrando como dispositivos conectados se tornaram o principal alvo de ataques cibernéticos, ressaltando que, ao deixar uma pequena "porta" aberta, há sempre alguém pronto para, em poucos segundos, coletar, utilizar e apagar todos os nossos dados para benefício próprio.

Att, Marinna

Att, Marinna