USJT – UC Sistemas Computacionais e Segurança – Prof. Calvetti - Atividade

A ANATOMIA DE UM ATAQUE IOT

Acácio

Daniel Silva

Matheus Bolato

Munir

CONTEXTO

- Durante as aulas de Sistemas computacionais e segurança, foi apresentada uma atividade de análise com o intuito de identificar, em uma produção áudio visual, as vulnerabilidades, tipos de técnicas utilizados pelo cracker e suas motivações.
- Link do vídeo: https://video-br.cisco.com/detail/video/5620318141001

RESUMO DO VÍDEO

O FBI prendeu um homem em San Francisco por invadir e atacar ciberneticamente um centro de pesquisa chamado Aupticon, que estava trabalhando no desenvolvimento de câmeras de rastreamento óptico para carros sem motoristas.

O criminoso começou pesquisando nas redes sociais pelos nomes de vários dos engenheiros que trabalhavam lá e durante a busca se deparou com uma liga de boliche onde várias empresas de tecnologia se reuniam às quartas-feiras. O estabelecimento era bem antigo e possuía um site bem ultrapassado, que continha os nomes das empresas e dos jogadores participantes.

O cracker invadiu o site do boliche com um ataque iFrame injection, infectando todos que entravam nele. Dessa maneira, após uma semana, o invasor teve acesso à rede da empresa por intermédio de um computador de um funcionário que foi infectado por esse malware.

Assim que se infiltrou na Aupticon, direcionou seu ataque para um termostato conectado à rede, explorando-o como um dispositivo vulnerável para manter acesso contínuo e expandir o alcance do ataque, pois não recebia vistoria da segurança.

Explorando a rede da empresa, percebeu que ela era muito simples e quase não tinha proteção. Ele encontrou vários arquivos do RH, documentos jurídicos, P&D e se deu conta de que poderia ganhar muito dinheiro com a venda dessas informações.

Após comercializar diversos registros da Aupticon para uma empresa rival por 75 bitcoins (I10.485 dólares na cotação atual 09/25), ele destruiu tudo, limpou tudo que encontrou, criptografou as unidades e excluiu os backups na tentativa de encobrir qualquer pista.

MOTIVAÇÃO

- O ataque foi movido por ganho financeiro, com recompensa paga pela empresa rival.

"Qcar vence a corrida - enquanto Aupticon luta para alcançá-la."

VULNERABILIDADES

1 - Identificação fácil de quem trabalha na Aupticon pelas redes sociais:

- A ausência da conscientização digital permitiu que perfis de funcionários fossem facilmente identificados em redes sociais, expondo informações que podem ser exploradas em ataques.

VULNERABILIDADES

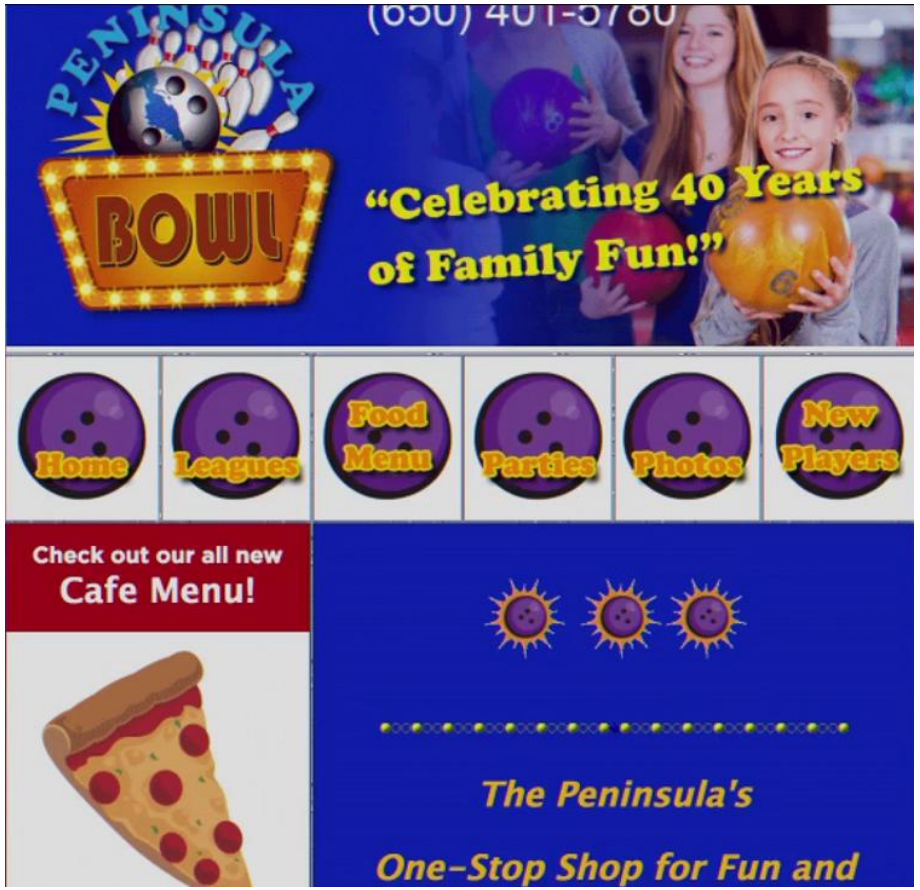
2 - O mesmo laptop que o funcionário usa em casa é o mesmo que ele usa na empresa:

- O uso do mesmo dispositivo em ambientes pessoais e corporativos representa uma falha do profissional, aumentando o risco de "contaminação" e comprometimento da rede corporativa por meio de vulnerabilidades exploradas em uso pessoais.

VULNERABILIDADES

3 - O site do boliche é ultrapassado e possui as informações dos funcionários e empresas de tecnologia:

- A utilização de um site desatualizado e a exposição de dados de colaboradores e usuários, representa um ponto crítico de vazamento de informações sensíveis.



VULNERABILIDADES

4 - A rede da Aupticon é muito simples, praticamente sem nenhuma segurança

- A infraestrutura de rede da Aupticon não tem camadas de proteção adequadas, apresentando-se como um ambiente sem monitoramento ou mecanismos de defesa, o que amplia significativamente a possibilidade de ataque.

Last Name	First Name	SSN	SEX	SALARY(ANNUAL)	PHONE	ADDRESS	
Sayton	Waverley	388-40-5524	Male	$145.89K	(495)596-2420	94	Kensington
Izhakov	Petra	703-53-7208	Female	$27.41K	(840)278-0777	831	Oxford
Bruyett	Malachi	858-62-7332	Male	$1.99M	(987)312-4286	18896	Grover
Claypool	Arron	478-22-4561	Male	$138.64K	(477)542-7343	9	Fairview
Tapner	Gerta	673-09-7658	Female	$27.13K	(784)799-4995	483	Randy
Gilffillan	Padraic	327-48-5610	Male	$1.68M	(709)209-1258	4	Carey
Presslee	Bev	449-26-4009	Male	$11.05K	(150)204-6750	07	Nobel
Hearley	Doloritas	216-95-4593	Female	$21.76K	(703)240-1215	9366	Bartillon
Lequeux	Dido	691-62-0544	Female	$18.74K	(876)654-2686	92	Meadow Vale
Semor	Nico	622-21-2107	Male	$221.65K	(622)111-2776	5	Mcguire
Gold	Cordy	549-03-9181	Female	$16.47K	(210)867-0958	35419	Reinke
McMorran	Emmy	674-81-0881	Female	$32.54K	(312)879-4221	1065	Algoma

TÉCNICAS DE ATAQUE UTILIZADAS

1 - Comprometimento inicial:

- O cracker invadiu o site da liga de boliche e fez um ataque iFrame Injection. Esse ataque consiste na inserção de um elemento HTML iframe malicioso em um site sem permissão, podendo permitir ataques como phishing, instalação de malware e roubo de dados.

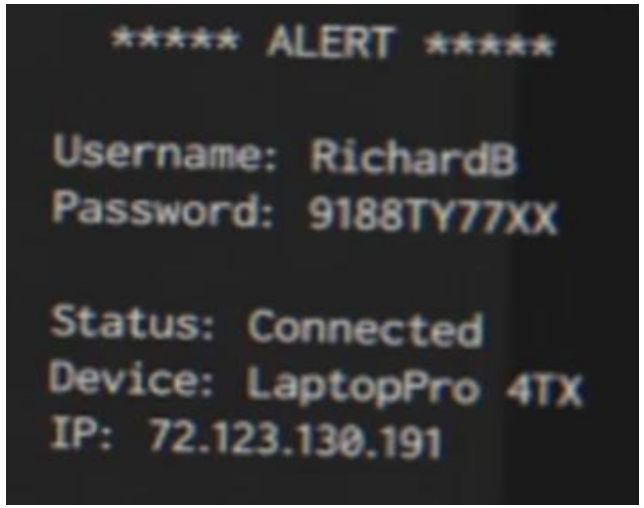
```
<iframe id="null" class="null">

class MedisploitModule < Msf::Exploit::Remote
  Rank = NormalRanking

  include Msf::Exploit::Remote::HttpServer::HTML
```

2 - Infecção de dispositivo:

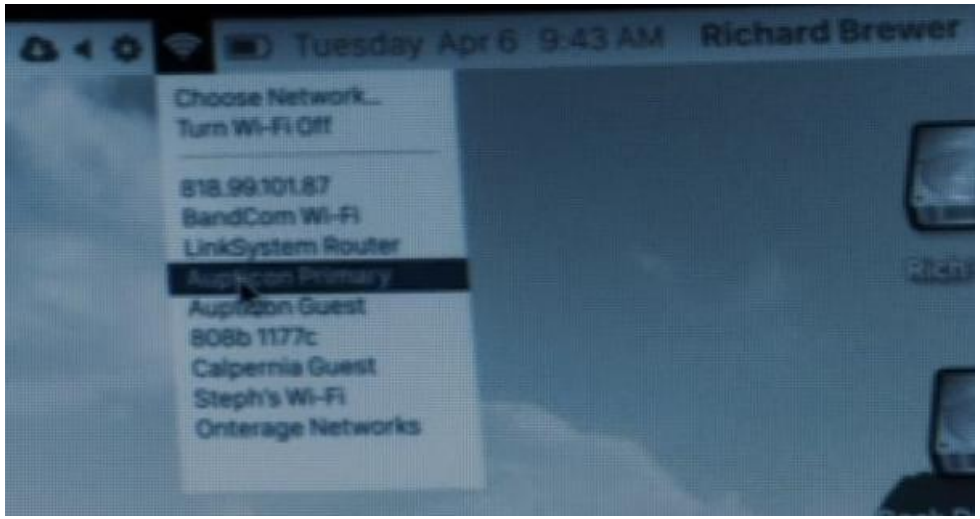
- Um funcionário da Aupticon acessou o site comprometido e teve seu laptop infectado.



TÉCNICAS DE ATAQUE UTILIZADAS

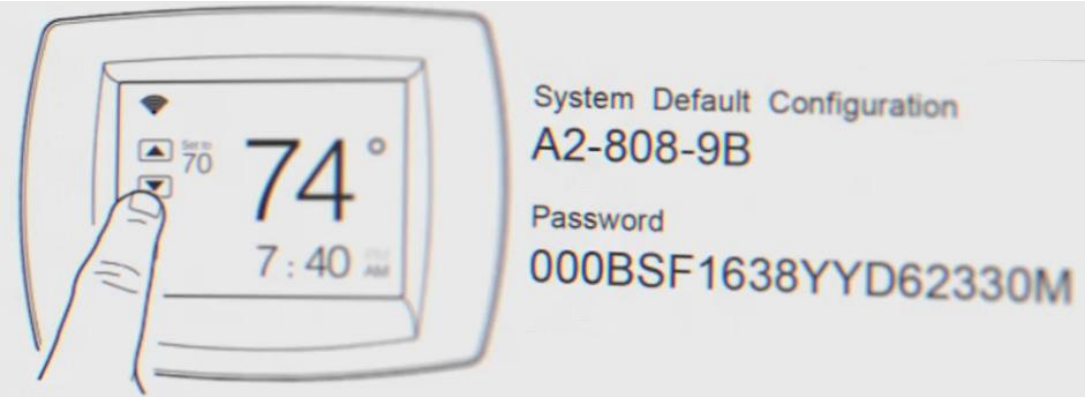
3 - Acesso à rede corporativa:

- Como o funcionário usava o mesmo laptop em casa e na empresa, o invasor obteve acesso inicial à rede da Aupticon.



4 - Exploração de IoT:

- O cracker comprometeu o termostato conectado à rede, ainda com senha padrão de fábrica, usando-o como ponto de persistência e movimentação lateral.



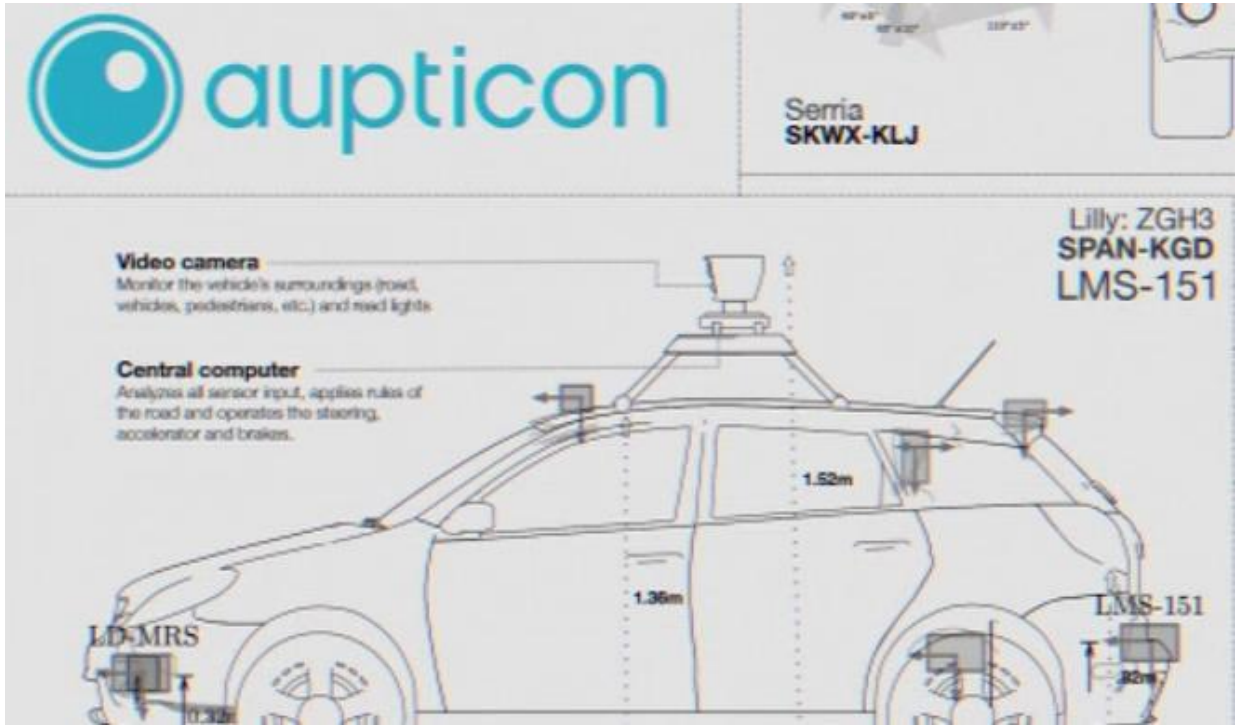
TÉCNICAS DE ATAQUE UTILIZADAS

5 - Exfiltração de dados:

- Documentos sensíveis foram copiados e vendidos para uma empresa rival.

6 - Acobertamento do crime:

- A fim de não ser encontrado, destruiu todos arquivos que conseguiu encontrar, criptografou as unidades e excluiu os backups da Aupticon.



FIM