Monumenta - Revista Científica Multidisciplinar

Artigos

Acesso sem controle a internet: Uma abordagem com engenharia social atraves de wireless fidelity (wifi)

Emanoel Guilherme Barros[1]

[1]União Brasileira De Faculdades – UniBF. Pós-Graduando Cybercrime e Cybersecurity: Prevenção e Investigação de Crimes Digitais

✉ e.guilherme.barros@outlook.com

Palavras-chave:
Wireless.
Internet.
Segurança.

Resumo

O atual contexto aborda aspectos teóricos e práticos que norteiam características e vulnerabilidades perigosas encontradas ao conectar em dispositivos na rede de computadores pública, ou seja, Wi-Fi grátis, que tem papel fundamenta de transmitir o sinal para qualquer dispositivo e assim como mostrar o perigo de passar informações a quais são dados sensíveis. As pesquisas foram feitas em locais como bar, restaurantes, shoppings e ônibus, onde ofertam Wireless grátis. Para identificação desses aspectos foram utilizadas ferramentas computacionais, pesquisa de campo e bibliográficas. A análise dos dados obtidas, através de criação de redes Wi-Fi pública com Acess Point falsa (FAKE AP). Com base em resultados obtidos sobre a pesquisa, os usuários submetidos a pesquisa, não desconfiaram que conectaram a uma rede falsa acessando com suas credenciais de uma rede social. O intuito da pesquisa foi mostrar aos leitores com quais tipos de perigos correm sem ao menos ter ideia do que pode acontecer com os seus dados, bem como alertá-los sobre a possibilidade de vazamento de seus dados na rede mundial de internet. Assim possibilitando também segurança a quem for ofertar internet grátis através de redes WiFi. Por fim acreditasse que existem poucas ferramentas eficaz, disponíveis e capazes de melhoras a segurança na rede de computadores.

Keywords:
Wireless.
Internet.
Security.

Abstract

The current context addresses theoretical and practical aspects that guide dangerous characteristics and vulnerabilities found when connecting to devices on the public computer network, that is, free Wi-Fi, which has the fundamental role of transmitting the signal to any device and as well as showing the danger to pass information to which is sensitive data. The surveys were carried out in places such as bars, restaurants, shopping malls and buses, where they offer free wireless. To identify these aspects, computational tools, field research and bibliographic tools were used. The analysis of the data obtained, through the creation of public Wi-Fi networks with false Access Point (FAKE AP). Based on results obtained on the survey, users submitted to the survey did not suspect that they connected to a fake network by accessing with their credentials from a social network. The aim of the research was to show readers what types of dangers they are in without even having an idea of what could happen to their data, as well as alerting them about the possibility of their data being leaked on the world wide web. Thus also enabling security to those who are going to offer free internet through WiFi networks. Finally, believe that there are few effective tools available and capable of improving security on the computer network.

1 INTRODUÇÃO

O Wireless Fidelity é o termo usado para descrever conexão sem fio em alta velocidade entre dispositivos móveis como laptops e a Internet. As redes Wi-Fi funcionam por meio de ondas de rádio. Elas são transmitidas por meio de um adaptador, o chamado “roteador”, que recebe os sinais, decodifica e os emite a partir de uma antena. Para que um computador ou dispositivo tenha acesso a esses sinais, é preciso que ele esteja dentro um determinado raio de ação, conhecido como hotspot. A ideia principal se refere ao uso de dispositivos móveis, seus serviços e recursos, que são capazes de descobrir nos ambientes outros dispositivos móveis, seus serviços e recursos e se conectar a eles.

No entanto, um dos grandes problemas de segurança acontece por não existirem cem por cento de segurança na interconexão de dispositivos nas redes. Por exemplo, os ataques de natureza externa são gerados de fora da rede, enquanto os ataques de natureza interna partem de dentro da rede e, por isto, são de mais difíceis prevenções. Analisando o cenário das empresas que fornecem redes Wi-Fi liberadas é possível afirmar que um usuário curioso com baixo conhecimento em segurança da informação ou até aqueles que não prestaram atenção ao que está fazendo assim podendo ser facilmente hackeado através de técnicas utilizadas por atacantes com intuito de obter informações de dados sensíveis, para realização de possíveis outros ataques com engenharia social e conseguir privilégios as quais não deveria ter do usuário que foi afetado.

O objetivo desse trabalho está relacionado ao seguinte tópico: Evitar o máximo possível que um invasor tenha sucesso ao tentar capturar seus dados através de acesso não autorizado utilizando engenharia social, deixando a rede vulnerável. De maneira que venha ter soluções simples e eficazes, tornando a rede mais segura. A solução será utilizar métodos para dificultar a ação maliciosa partindo de um atacante, algumas medidas podem ser tomadas, como não acessar qualquer rede disponível, não colocar as credenciais em qualquer local que for acessar internet e outros.

Por fim, apresentar algumas considerações sobre WiFi na tecnologia e sua insegurança tecnológica. Apresenta também um elo importante para nos aproximar das técnicas utilizadas por invasores, evidenciando as relações entre educação com a tecnologia. Discutir insegurança da tecnológica não apenas como preparação para preencher as necessidades do usuário, colocando o conceito de tecnologia segura, com base nestas considerações, numa nova perspectiva que passa pela análise de em tráfego de rede e o perigo alheio. Existem maneiras de evitar tais acontecimentos, dependendo da tecnologia a ser implantada por profissionais da área de segurança capazes de gerenciar políticas e regras de segurança. Atualmente com o avanço e crescimento da tecnologia e com a facilidade de acesso por qualquer tipo de usuário, isso se torna um grande risco.

2 ENGENHARIA SOCIAL

É o termo utilizado para descrever o método de ataque, onde o invasor faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores, dispositivos ou informações privilegiadas.

O hacker norte-americano Kevin Mitnick ficou famoso na década de 60, por conseguir informações secretas de grandes empresas dos Estados Unidos apenas telefonando para alguns funcionários e, após conquistar a confiança deles, fazendo algumas perguntas, assim obteve com êxito a invasão de sistemas e locais sem permissão ou autorização alguma. Kevin Mitnick defende, em seu livro, A Arte de Enganar (2003), que concluiu ser mais fácil descobrir a senha do usuário simplesmente perguntando, ao invés de utilizar-se de artifícios tecnológicos elaborados.

Figura 1

Imagem retirada do site de busca www.google.com (autor desconhecido)

Em tempos como hoje, é inegável o uso das tecnologias para execução das mais variadas tarefas. Este ambiente digital, além de trazer benefícios, trás também muitos riscos para as corporações (MACIANO, 2006).

E se naquela já era possível conseguir informações dos próprios usuários a fornecerem informações como, nome, setor ou até senha de acesso por telefone, hoje, com as redes sociais é ainda mais fácil enganar as pessoas e conseguir dados valiosos.

3 WIRELESS FIDELITY

Wi-Fi é a abreviação dada para a palavra Wireless Fidelity(), ou seja, termo usado para descrever conexão sem fio de alta velocidade em distância curta, entre dispositivos para acesso a rede de computadores como, smartphones, notebooks smartTVs e outros.

Figura 2

Imagem retirada do site de busca www.google.com (autor desconhecido)

Esse tipo de conexão normalmente é ofertado por roteadores, ou seja, a peça fundamental para que seja liberado o sinal do Wi-Fi com limite a uma determinada área de distância assim conectando vários dispositivos ao mesmo tempo de uma única vez.

Figura 3

Imagem retirada do site de busca www.google.com (autor desconhecido)

4 METODOLOGIA

Acesso as informações através de Acesse Point falso (Fake AP). Atualmente é comum encontrar ferramentas e sites com tutorias, ensinado utilizar, de modo geral, para qualquer tipo de usuário que deseje aprender a manusear a ferramenta Wifiphisher para coletas de dados.

Para esse tipo de coleta foi utilizado a implementação de um Honeypot (pote de mel) que consiste em sistema operacionais (S.O.) Linux como por exemplo, utilização do Kali Linux na versão 2020.1 com objetivo de utilizar algumas de suas ferramentas na criação de sondagem passiva e ativa, tentativas de desautenticação de clientes e autenticação, assim como na rede falsa através da ferramenta Wifiphisher ou outra qualquer que seja capaz de obter o mesmo resultado.

Figura 4

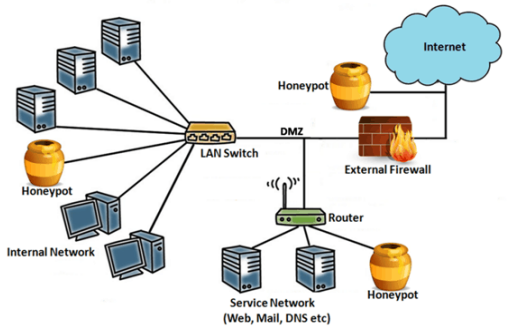

Imagem retirada do site de busca www.google.com (autor desconhecido)

No site https://osintbrasil.blogspot.com/2018/10/wifiphisher.html qualquer usuário encontrará o passo a passo da utilização da ferramenta Wifiphisher para captura de login e senha de acesso a página como Facebook, vale lembra que para tal processo o usuário deve ter algum conhecimento sobre redes de computadores.

5 RESULTADOS

Ao levantar o serviço da rede falsa para captura de informações em locais públicos com o mesmo nome da rede original é surpreendente o número de usuários que dão seus dados (chegam a conectar ao ponto de acesso não confiável) só para ter acesso a internet a qual eles não imaginam que estão sendo monitorado em tempo real por um invasor para utilização e intenção de fazer o mal após a coleta de dados sensíveis.

Para um mal-intencionado na rede, a coleta será em tempo de segundos, por ter facilidade de se conectar na rede verdadeira fazer a desautenticação dos usuários a rede verdadeira e ao levantar a rede falsa pegar dos usuários informações para acesso como senha sendo seu login e senha de redes sociais.

6 CONCLUSÃO

Assim podemos concluir que, em determinados locais será de inteira responsabilidade dos usuários fornecer informações para acesso à internet em redes públicas. Vale ressaltar que o perigo é real e imperceptível para o usuário ao ingressar a rede sem fio. Sempre desconfie do acesso grátis, lembrando que você será prejudicado e muitas vezes irreversível a perca dos dados com graves lesões como, por exemplo, fraudes em seu nome, difamação, conteúdo inapropriado será publicado em suas redes sociais sem suas permissões, danos morais, danos financeiros e outros. Para comprovar e recuperar suas informações muitas vezes não é tão simples, pois sem comprovação do que houve a dificuldade é maior para provar que você não fez ou não é culpado por um ato o qual você que está sendo acusado. Por fim uma

das melhores maneiras de se conectar a uma rede em locais públicos é através de dados moveis, podendo ser comprado nas operadoras ou compartilhado por amigos que estão no mesmo local o qual o usuário deseja acessa a internet e lembrando que ao compartilhar deve-se colocar um nome a rede e uma senha personalizada fazendo uma mistura com caracteres especiais como símbolos, letras maiúsculos e minúsculos e números.

REFERÊNCIAS

Disponível em: https://cio.com.br/conheca-seis-das-tecnicas-de-engenharia-social-muito-eficazes/ Acessado em 10/07/2020.

Disponível em: https://osintbrasil.blogspot.com/2018/10/wifiphisher.html Acessado em 12/07/2020.
Disponível em: https://www.kali.org/, acessado em 16/07/2020.

MARCIANO, João Luiz Pereira. **Segurança da Informação – uma abordagem social.** 2006. Monografia. Disponível em http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%2 0Marciano.pdf

MITNICK, Kevin D; Simon, William L. **A Arte de Enganar**. São Paulo: Blucher, 2003. p. 25.