UNIVERSIDADE CATÓLICA DE PELOTAS
ENGENHARIA DE COMPUTAÇÃO
Redes de Computadores

Gabriel Harter Zoppo

Backdoor,Phishing e Spoofing

Pelotas,
29/10/2021

1. Backdoor:

1.1 Definição:

Backdoor é um método não documentado de entrada em sistemas (software, plataformas, dispositivos etc.) que pode ser usado de forma legítima por fabricantes para restaurar acessos.

Backdoor é uma porta de acesso ao sistema, que foi criada a partir de um programa instalado que não foi autorizado pelo proprietário do sistema e que permite o acesso ao computador por pessoas não autorizadas.

1.2 Usos:

- Polícia e órgãos de justiça.
- Desenvolvedores do Software ou dispositivo(Suporte técnico).
- Crackers

1.3 Como é obtido:

- Downloads de aplicativos piratas.
- Emails
- Senhas fracas

1.4 Como se proteger:

- Monitore a atividade da rede.
- Invista em uma boa solução de cibersegurança.
- Aposte em senhas fortes:
- Cuidado ao escolher aplicações e plugins confiáveis:

2. Phishing:

2.1 Definição:

Phishing é um termo originado do inglês (fishing) que em computação se trata de um tipo de roubo de identidade online. Essa ação fraudulenta é caracterizada por tentativas de adquirir ilicitamente dados pessoais de outra pessoa, sejam senhas, dados financeiros, dados bancários, números de cartões de crédito ou simplesmente dados pessoais.

O phishing é um dos golpes mais antigos e conhecidos da internet. Podemos definir phishing como qualquer tipo de fraude por meios de telecomunicação, que usa truques de engenharia social para obter dados privados das vítimas.

2.2 Tipos:

Phishing por e-mail: De longe, o método mais comum, o phishing por e-mail usa o e-mail para introduzir a isca de phishing. Esses e-mails geralmente contêm links que levam a sites maliciosos ou anexos que contêm malware. Posteriormente, vamos mostrar como é um e-mail de phishing, para você saber quais devem ser evitados.

Phishing nos sites: Os sites de phishing, também conhecidos como sites falsificados, são cópias falsas de sites reais conhecidos e confiáveis. Os hackers criam esses sites falsificados para fazer você inserir suas credenciais de login, que podem ser usadas para fazer login nas suas contas reais. Os pop-ups também são uma fonte comum de phishing nos sites.

Vishing: Abreviação de “phishing de voz”, vishing é a versão em áudio do phishing na internet. O golpista tentará convencer as vítimas por telefone a divulgar informações pessoais que podem ser usadas posteriormente para roubo de identidade. Muitas chamadas automatizadas são tentativas de vishing.

Smishing: Smishing é phishing via SMS. Você recebe uma mensagem de texto que solicita clicar em um link ou baixar um aplicativo. Mas, ao fazer isso, você baixará malware no seu telefone, que poderá roubar suas informações pessoais e enviá-las ao invasor.

Phishing nas redes sociais: Alguns invasores podem acessar contas de redes sociais e forçar as pessoas a enviarem links maliciosos para seus amigos. Outros criam perfis falsos e usam esses perfis para phishing.

2.3 Como se proteger:

- Mantenha-se informado
- Desconfie
- Confirme antes de agir
- Verifique os certificados de segurança
- Altere as senhas regularmente
- Verifique suas contas
- Use um bloqueador de anúncios
- Leia e-mails como texto sem formatação

3. Spoofing:

3.1 Definição:

O spoofing é semelhante ao phishing, em que o invasor rouba a identidade do usuário lícito e se finge de outro indivíduo ou organização com intenção mal-intencionada, a fim de violar a segurança do sistema ou roubar as informações dos usuários.

Spoofing é um termo amplo para o tipo de comportamento em que um criminoso virtual se disfarça como um usuário ou dispositivo confiável para que você faça algo que beneficie o hacker e prejudique você.

3.2 Comparação entre Phishing e Spoofing:

Base para comparação	Phishing	Spoofing
Basic	O scammer de phishing falsifica organizações e pessoas confiáveis para ganhar a confiança de seus alvos e roubar informações.	Os fraudadores fraudulentos não estão necessariamente tentando roubar qualquer informação, mas podem estar tentando atingir outras metas maliciosas.
Relação	Os ataques de phishing podem usar spoofing como estratégia.	Spoofing não é necessariamente phishing.
Processo	O phishing é acompanhado de roubo de informações.	Spoofing não requer necessariamente roubo de informações.
Realiza	Recuperação	Entrega

3.3 Tipos:

Spoofing de e-mail/chamadas/sms: Provavelmente o mais comum, mas não quer dizer não pessoas que caiam. Esse método consiste em e-mails, ligações e sms falsos se fazendo passar por uma empresa. Geralmente esses contatos são enviados com mensagens em tons mais agressivos no intuito da vítima tomar decisões mais rápidas sem ao menos sem ela realmente deveria receber aquele e-mail.

Spoofing de DNS: Quando alterado o DNS do roteador, o cibercriminoso pode desviar acessos desejados pelo usuário por um site falso. Nestas cópias de sites, o usuário pode acabar tendo os dados roubados ou baixar malwares sem saber.

Spoofing de site: Nesse caso o cibercriminoso cria um site falso para enganar usuários desatentos que estejam buscando o de uma outra empresa. Geralmente os criminosos que praticam essa ação dão preferência a sites de compra e banco, onde é necessário colocar dados para compra. Quando acessado esses dados, fica ainda simples para aplicar prejuízo financeiro à vítima.

Spoofing ID: Esse método consiste em clonar um telefone para acessar contas e redes sociais das vítimas. Essa ação pode ser usada para burlar sistema de autenticação de dois fatores, a vítima pode acabar perdendo o WhatsApp, por exemplo.

Spoofing de IP: Muito usado em ataques de DDoS, este método permite ao criminoso virtual alterar o endereço IP legítimo de um dispositivo em uma rede fechada, enganando os demais, deixando-os expostos.

3.4 Como se proteger:

- Use um software antivírus
- Fique atento
- Entre em contato para confirmar
- Troque de senha regularmente
- Informe as tentativas de spoofing

4. Referências:

4.1 Backdoor:

https://www.blockbit.com/pt/blog/como-evitar-backdoors/
https://backupgarantido.com.br/blog/malware-backdoor/
https://www.vcptec.com.br/2019/04/24/o-que-e-um-backdoor/
https://www.youtube.com/watch?v=qU5hn5eXcHY

4.2 Phishing:

https://canaltech.com.br/seguranca/O-que-e-Phishing/
https://www.avast.com/pt-br/c-phishing
https://www.youtube.com/watch?v=mpXZo5ifYss

4.3 Spoofing:

https://www.combateafraude.com/post/saiba-o-que-e-spoofing-e-como-se-defender
https://pt.gadget-info.com/difference-between-phishing
https://www.kaspersky.com.br/resource-center/definitions/ip-and-email-spoofing
https://www.youtube.com/watch?v=8i-WMK22lrg