

CUIDADO: Como os hackers descobrem as senhas das vítimas?



Métodos variam entre phishing, instalação de malwares na máquina alvo e testadores automáticos de senha; saiba mais.

Ataques hackers são sempre inconvenientes porque propagam a sensação de insegurança nas vítimas, e ainda abrem brechas para que os cibercriminosos roubem dados preciosos e os vendam na internet ou os utilizem para cometer mais crimes.

Como os hackers descobrem as senhas das suas vítimas?

De forma geral, há inúmeras maneiras para conseguir a senha de outra pessoa e invadir a sua conta. No entanto, estas estratégias, geralmente, se dividem em dois grupos de ações: utilização de programas automatizados para testar senhas ou pela instalação de malwares na máquina da vítima.

No primeiro caso, o usuário utiliza um programa específico que acessa uma plataforma da web (sites, provedores de e-mail, redes sociais, bancos, etc.), e este software testa, de forma autônoma, diferentes combinações para nomes de usuários e senhas. Após descobrir o endereço de e-mail, por exemplo, o hacker se foca em descobrir a senha para então acessar o perfil da vítima.

Esses 'testadores de senhas' costumam funcionar quando as vítimas detêm senhas fáceis ou com algum encadeamento lógico. Ou seja, senhas com números em sequência, com endereços residenciais, números de CPF e RG, e datas de nascimento. Senhas formadas por palavras e frases também são um prato cheio. Seja como for, o programa testa inúmeras combinações possíveis, porque seu banco de dados possui uma lista enorme com as senhas mais comuns, e ele não para até descobrir a combinação perfeita que permitirá uma invasão.

No segundo caso, é necessário instalar um malware na máquina da vítima. A palavra 'malware' é um termo generalista que designa qualquer programa malicioso cujo objetivo é espionar, infectar ou roubar informações de uma pessoa. Seguindo esse raciocínio, o cibercriminoso utiliza várias estratégias para convencer a vítima a clicar em um link suspeito ou anúncio suspeito, ou a baixar um arquivo.

Uma vez que isso acontece, a ação do hacker vai depender do tipo de malware instalado: se for um spyware, ele poderá gravar áudio e imagens da tela da sua máquina; já um keylogger grava as teclas que você utiliza para digitar a senha, que posteriormente será roubada.

Independentemente da estratégia utilizada -- e há muitas outras além destas que citamos -- o objetivo sempre será o mesmo: conseguir a sua senha e nomes de login, e adquirir as suas informações. Uma vez que isso acontecer, eles podem se passar por você ao contatar outras pessoas,

vender seus dados na darknet, extorqui-lo para devolver os dados, e até utilizá-los para realizar mais crimes.

E como se prevenir?

Utilize senhas fortes, com 12 caracteres ou mais, e que contenham números, letras maiúsculas e minúsculas, e símbolos especiais;

Use autenticação de dois fatores com um aplicativo próprio, como o app Authy;

Não clique em links ou anúncios suspeitos, nem baixe qualquer arquivo pela internet;

Não responda nem abra mensagens de e-mail com endereços esquisitos, cheios de números e letras;

E se receber qualquer tipo de cobrança, verifique se você realmente possui um cadastro no local da cobrança, e se sim, pesquise na internet os números oficiais do SAC para entrar em contato. Não atenda nem responda ligações, e-mails e SMS enviados para você para 'confirmar' compras realizadas, sempre opte por entrar em contato com o SAC.

Foto: Divulgação

<https://jornalpanfletus.com.br/noticia/5152/cuidado-como-os-hackers-descobrem-as-senhas-das-vitimas> em 04/07/2024 05:20