COMO SE DEFENDER DE ATAQUES DE CRACKERS NA INTERNET?

Primeiramente, vamos esclarecer que hackers são aqueles que utilizam de seus conhecimentos especializados para modificar tanto softwares como hardwares e adicionar novas funções nas aplicações. Eles têm a capacidade de resolver problemas complexos de segurança, contudo, sempre para trazer benefícios. Já os crackers são aqueles com intenções maliciosas e criminosas, são eles que quebram a segurança de softwares para praticar ações que prejudicam sistemas, pessoas e empresas, desde prejuízos financeiros até morais e de confidencialidade governamental e bancárias. Portanto, é importante não confundir os termos. Quando alguém entrar no assunto com você, não deixe de explicar o verdadeiro significado dos dois termos. Existem inúmeros casos de ataques de crackers que repercutiram na mídia, mas ainda são noticiados como hackers.

Um caso noticiado em 2016 (ALENCAR, 2016), mostra que crackers conseguiram dados de e-mail, tipo de conta, país de origem e data de renovação da conta de usuários do Spotify. Como eles conseguiram? Simples, eles desenvolveram páginas web ou aplicativos idênticos aos oficiais e o usuário que não percebe a diferença no endereço do site, por exemplo, acaba por realizar o login nessa página. E dessa forma darão acesso às suas informações para os invasores que puderam acessar, por exemplo, as contas pagas de usuários. Neste caso, os usuários perceberam que havia músicas marcadas como ouvidas, mas que eles nunca haviam ouvido.

Outro caso recente (LOUBACK, 2018), de 2018, relatou a ação de um malware chamado CamuBot. Esse malware se camufla como um módulo de segurança que é exigido ser instalado no computador pelos bancos. O CamuBot atacou usuários corporativos e organizações do setor público. Como conseguiram? Os invasores ligavam para as empresas dizendo que eram funcionários do banco e os convenciam de que era necessário atualizar o software de proteção do banco. Ao instalar o software malicioso, o computador é contaminado com um bot capaz de roubar senhas de bancos, inclusive burlando mecanismos considerados eficientes de autenticação. Este caso não se tratou de um golpe qualquer, pois o CamuBot possibilita o controle do dispositivo de forma remota pelo cracker, além da interface de instalação do programa ser idêntico ao original. O cracker tem acesso ao computador da vítima e, portanto, da sua conta bancária, o que engana e dificulta reconhecer que não é o próprio correntista. Outra característica é que o malware considerou a engenharia social, ou seja, analisou, inclusive, redes sociais das vítimas e então o golpe, que se inicia por telefone, foi personalizado para cada um, pois assim se descobre quem é o dono da empresa e quem teria o acesso às informações das contas.

Referências

ALENCAR. F. Hackers roubam milhares de senhas do Spotify; veja como mudar a sua. TechTudo, 26 abr. 2016, Notícias. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2016/04/hackers-roubam-milhares-de-senhas-do-spotify-veja-como-mudar-sua.html>. Acesso em: 1 jul. 2019.

LOUBACK, A. L. Golpe com vírus CamuBot usa nome de bancos e faz vítimas no Brasil. TechTudo, 6 set. 2018, Notícias. Disponível em: <https://www.techtudo.com.br/noticias/2018/09/golpe-com-virus-camubot-usa-nome-de-bancos-e-faz-vitimas-no-brasil.ghtml>. Acesso em: 1 jul. 2019.

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

**Unidade 1 – Serviços de Redes de computadores**

*Vamos praticar  
Muitos ataques maliciosos são desenvolvidos por crackers burlando novos mecanismos de autenticação e segurança. Você percebeu que os ataques mais sofisticados envolvem não somente ações digitais, como contatos por telefone e análise de redes sociais, isto é, uma interação entre invasor e vítima? Pesquise ataques diferenciados e crackers famosos, analise suas ações maliciosas e responda, em até dois parágrafos:  
Como podemos tentar nos defender desses ataques, considerando tanto a utilização de mecanismos de autenticação como também atitudes de segurança?  
Não se esqueça de compartilhar suas conclusões no fórum da seção “Compartilhe”.*

No uso de computadores para fins pessoais os mecanismos de proteção já são velhos conhecidos da grande maioria dos usuários porém, muitas vezes ignorados, principalmente quando existe o desejo de obter softwares sem pagar pela sua licença. Ações como nunca fazer o download e executar softwares de origem desconhecida ou duvidosa, verificar a segurança das páginas onde são preenchidos formulários com dados pessoais e não compartilhar conteúdo sensível através de plataformas sem criptografia ou com pessoas não confiáveis.   
 Em smartphones, que já são vetores de grande importância em transações bancárias, podemos utilizar em nosso favor os mecanismos de autenticação biométrica e de dois ou mais fatores, estes também estão disponíveis em desktops porem com maior frequência nos celulares inteligentes. Já na segurança de dados das empresas o cuidado deve ser muito maior, recentemente posta em vigor, a LGPD vem ajudar a manter os dados dos usuários seguros se bem aplicada. O uso de softwares de controle de acesso a dados e um sistema robusto de segurança devem ser dinâmicos e sempre atualizados às novas ameaças.

Referências:  
<https://www.perallis.com/news/maiores-ataques-hackers-da-historia>  
<https://www.controle.net/faq/ataque-ransomware-tudo-o-que-voce-precisa-saber>

@icsalgado - <https://www.linkedin.com/in/icsalgado/>

Feedback:  
Caro estudante,

Ao analisar alguns ataques noticiados e atitudes de crackers famosos, você verá que, com o passar dos anos, governo, bancos e próprias pessoas estão tomando mais cuidado quanto a isso. Empresas e profissionais de TI têm desenvolvido novos mecanismos e técnicas de autenticação e segurança da informação para que ações maliciosas sejam cada vez mais evitadas. Esses mecanismos incluem algoritmos de criptografia para que os dados confidenciais trafeguem codificados e sejam decodificados apenas no destino por chaves e pessoas que tenham autoridade para fazer isso. Outros mecanismos podem envolver solicitação de mais de um fator para autenticar o usuário, tal como, além de uma senha, um token ou mesmo uma digital. Os mecanismos de dois ou mais fatores têm se mostrado eficientes atualmente.

Sobre as atitudes, vimos que os criminosos não são apenas aqueles que sabem manipular a informática, mas também aqueles que sabem persuadir as vítimas, especialmente por telefone. Por exemplo, um caso recente mostrou que o criminoso liga para a vítima dizendo que é do banco e pergunta se ela fez determinadas compras no cartão de crédito – que, obviamente, ela não fez, pois são inventadas – então a pessoa prontamente se assusta e diz que não fez as compras. O criminoso diz que ela deve ligar para o número que está no verso do seu cartão para cancelá-lo. O criminoso finge que desliga e a vítima digita o número do banco, enquanto isso, o criminoso está, através de um aplicativo no computador, captando tudo o que a vítima digita. Agora, o criminoso sabe qual é o banco da vítima (pelo número digitado) e prontamente solta uma gravação do respectivo banco. Essa gravação parece verídica e automaticamente vai pedir informações como número do cartão e senha. A pessoa informa digitando no telefone, pois realmente acredita que ligou para o banco. O aplicativo do criminoso capta tudo o que foi digitado e assim a vítima tem os dados do seu cartão roubados. Essa atitude mostra que a vítima não tem o conhecimento de que os bancos jamais ligam para seus clientes para pedir sua senha. Provavelmente, se ela recebesse um e-mail com um pishing, poderia clicar no link enviado acreditando que o site era realmente do banco, pois esses geralmente são idênticos aos originais. Nesse caso, é necessário analisar o link acessado e, antes de tudo, saber que bancos também não enviam e-mail pedindo para redefinir senha ou preencher qualquer formulário com seus dados pessoais e confidenciais. Qualquer contato que façam envolvendo banco, devemos ficar atentos e sempre averiguar adequadamente o procedimento, e jamais fornecer senhas.