A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

CEO Impostor / BEC

O que é CEO Impostor / BEC?

Os atacantes cibernéticos continuam a desenvolver um ataque chamado CEO Impostor ou Comprometimento de Email Empresarial (BEC, Business Email Compromise). São ataques direcionados de email que conduzem a vítima a tomar uma ação que não deveriam. Em muitos casos os atacantes estão em busca de dinheiro. O que torna esse ataque muito perigoso é que os atacantes pesquisam suas vítimas antes de lançar o ataque. É também muito difícil para tecnologias de segurança pararem esses ataques porque não há um anexo infectado ao email ou links maliciosos para detectar. Aqui está a forma como o ataque funciona:

O atacante cibernético utiliza a Internet para pesquisar sua vítima intencional e as pessoas com quem sua vítima interage. Por exemplo, se te escolherem como alvo, irão pesquisar quem é seu chefe no trabalho ou talvez um corretor com quem esteja negociando de casa. O atacante cibernético então monta um email, fingindo ser uma dessas pessoas e o envia a você. O email é urgente, requer que você tome uma ação imediata, como pagar um boleto, mudando o receptador do pagamento. Ou tenta convencer você a responder enviando arquivos sigilosos. O email funciona pressionando-o para fazer o que querem. Aqui vão dois exemplos de como um ataque desses pode acontecer:

Transferência Bancária: Um criminoso cibernético está atrás de dinheiro. Eles pesquisam a companhia onde você trabalha, por exemplo identificando quem trabalha no Contas a Pagar ou qualquer pessoa responsável por transferências monetárias. Os criminosos então montam e enviam um email para esses indivíduos fingindo ser o respectivo chefe ou um executivo sênior. O email diz a eles que há uma emergência e é necessário fazer uma transferência imediata para uma nova conta bancária. O email pressiona o leitor a cometer um erro que, na verdade, será o envio de dinheiro para o criminoso cibernético;

Fraude de Impostos: Criminosos cibernéticos estão em busca de informações pessoais para utilizar em fraude de impostos. Uma das formas mais rápidas para obter essas informações é roubá-las de todos os funcionários de uma empresa. Os criminosos cibernéticos pesquisam e identificam quem trabalha no Recursos Humanos. Então enviam emails falsos para esses indivíduos, fingindo ser um executivo sênior ou talvez alguém do departamento jurídico. O email cria uma estória urgente, dizendo que as informações sobre impostos de todos os funcionários devem ser enviadas imediatamente. As pessoas do Recursos Humanos pensam que estão enviando documentos sigilosos para um executivo sênior, quando na verdade estão enviando para um criminoso cibernético.

Protegendo-se

Então o que você pode fazer para se proteger ? Bom senso é a sua melhor defesa. Aqui estão as pistas mais comuns a procurar:

- **O email é muito curto e urgente (frequentemente apenas algumas sentenças) e a assinatura diz que o email foi enviado de um dispositivo móvel;**
- **Há um forte senso de urgência lhe pressionando para ignorar ou desconsiderar as políticas da sua empresa. Sempre siga as políticas e procedimentos do seu trabalho, mesmo que o email pareça ter vindo do seu chefe ou mesmo do CEO;**
- **O email é sobre trabalho mas utiliza uma conta de email pessoal, como @gmail.com ou @hotmail.com;**
- **O email parece ter vindo de um líder sênior, colega de trabalho ou terceiro que você conhece ou com quem trabalha, mas o tom da mensagem não parece com o deles;**
- **Fornece instruções de pagamento e elas divergem das que você já havia recebido, como por exemplo a exigência de um pagamento imediato para uma conta bancária diferente.**

Se você suspeita ter sido alvo de um ataque com alvo, pare toda a interação com o atacante e relate ao seu supervisor. Se você já foi alvo em casa ou já foi vítima e fez uma transferência bancária, relate imediatamente ao seu banco e, então, aos órgãos de justiça.

Editor Convidado

Don Cavender *é um Agente Especial do FBI aposentado, com mais de 22 anos de experiência em forense computacional e crime cibernético. Recentemente tem trabalhado como Coordenador BEC em Washington DC, focando em organizações de crime cibernético. Ele ministra treinamentos e conduz pesquisas em forense digital e investigações cibernéticas.* @don_cavender
https://www.linkedin.com/in/donald-cavender

Recursos

Engenharia Social:	https://www.sans.org/u/HE3
Pare esse Phishing:	https://www.sans.org/u/HE8
Pare aquele Malware:	https://www.sans.org/u/HEd
Pare aquele Malware:	https://www.sans.org/u/HEi