Two-Step Phishing Attacks

Two-step phishing attacks are on the rise as threat actors become more sophisticated in targeting potential victims and evading detection. These phishing attacks use legitimate vendors that the threat actor has previously compromised. The threat actor will monitor personal accounts at the compromised organization to build a potential victim list. The victim list includes current customers that are expecting to receive an email from the compromised vendor in regard to DocuSign, order details, invoice, or tracking information among others. Due to the threat actor having access to organizational email accounts, they can develop a malicious email with the same syntax and aesthetics as an actual email from the vendor. The threat actors further reduce detection capabilities by using the same applications as the vendor. If the vendor requires a Microsoft login, the initial link provided in the malicious email that the victim clicks on will redirect to a fake Microsoft login page for the victim to input credentials. It is at this stage that the victim has a chance to detect if they are inputting their credentials into a secure Microsoft Login page or if it is a fake page by looking at the URL.

These types of phishing attacks are largely successful as the threat actor is relying on the credibility of the compromised vendor to carry out the phishing attack. The victim is less cautious when prompted for credentials, credit card information, or other sensitive data. It is critical that individuals confirm URL addresses before entering credentials, as these phishing campaigns will originate from legitimate corporate emails. Organizations and individuals should also consider implementing multi-factor authentication (MFA) in addition to the steps outlined above. MFA can provide an extra layer of protection against phishing attacks, even if the attacker is able to obtain the victim's credentials. Companies should remain vigilant and take appropriate steps to protect themselves and their employees from these types of threats, including implementing strong cybersecurity measures, investing in employee training and awareness, and regularly updating their security protocols.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.

References:

1. https://www.helpnetsecurity.com/2023/03/16/how-two-step-phishing-attacks-evade-detection-video/