Issued 1/12/17

Highly Effective Gmail Phishing Technique Now Circulating

A new highly effective phishing technique targeting Gmail and other services has been gaining popularity during the past year among attackers. Over the past few weeks there have been reports of experienced technical users being hit by this.

This attack is currently being used to target Gmail customers and is also targeting other services.

The way the attack works is that an attacker will send an email to your Gmail account. That email may come from someone you know who has had their account hacked using this technique. It may also include something that looks like an image of an attachment you recognize from the sender.

You click on the image, expecting Gmail to give you a preview of the attachment. Instead, a new tab opens up and you are prompted by Gmail to sign in again.

Once you complete sign-in, your account has been compromised. A commenter on Hacker News describes in clear terms what they experienced over the holiday break once they signed in to the fake page:

"*The attackers log in to your account immediately once they get the credentials, and they use one of your actual attachments, along with one of your actual subject lines, and send it to people in your contact list. For example, they went into one student's account, pulled an attachment with an athletic team practice schedule, generated the screenshot, and then paired that with a subject line that was tangentially related, and emailed it to the other members of the athletic team.*"

The attackers signing into your account happens very quickly. It may be automated or they may have a team standing by to process accounts as they are compromised.

Once they have access to your account, the attacker also has full access to all your emails including sent and received at this point and may download the whole lot.

Now that they control your email address, they could also compromise a wide variety of other services that you use by using the password reset mechanism including other email accounts, any SaaS services you use and much more.

This phishing attack designed to steal usernames and passwords on Gmail is being used right now with a high success rate.