Issued 3/16/17

Dangerous New Gmail Phishing Attack can Easily Steal your Google Login

Why are the Windows and Android platforms always targeted by malware and other malicious attacks from nefarious hackers? Because they're used by so many people that the odds of a successful attack are dramatically increased compared to less popular platforms like macOS. For that same reason, Google's Gmail service is often the target of phishing scams that have become increasingly effective in recent years.

Now, a new scam has been uncovered that may very well be the most well-executed scam in recent history, making it all too easy for victims to have their Google login credentials stolen. Via Lifehacker, the cyber security experts at Wordfence first brought this new scam to light earlier this year. In a nutshell, the scam targets Gmail users who access their email accounts in a web browser. It displays a graphic that looks identical to the graphic Google uses to indicate a PDF or Word document attachment, but it embeds the image in the email body itself. When the user clicks on it, he or she is redirected to a page that looks just like the normal Google login screen.

While the look is spot on, the page isn't actually hosted on Google's servers. Instead, it's a recreation of the Google sign-in page that steals a user's login credentials as he or she inputs a username and password. Those credentials are then used to gain access to the victim's Gmail account and further spread the

scam. The nearly identical resemblance to Google's own attachment graphics and login page is what makes this scam so dangerous. In fact, the only way most people are able to spot it is if they notice that the URL of the login screen that opens after the fake attachment is clicks begins with "data:text/htyml" rather than "https:" as it should. This is because the fake login page isn't actually hosted on a secure server.

As noted in an update from Wordfence, the latest version of Google's Chrome browser now displays a "Not Secure" warning when pages like this load, which should help many users to avoid falling victim to the scam. Not everyone uses Chrome, however, and not all users who do browse with Chrome actually install Google's updates.