Google Docs comment feature exploited to distribute phishing links

January 7 2022, by Bob Yirka

Credit: Unsplash/CC0 Public Domain

A team of security researchers at Avanan is reporting that hackers are taking advantage of a Google Docs security vulnerability—one that takes advantage of a comment feature. They are claiming that they saw

hackers using the vulnerability to target 500 inboxes of 30 Outlook users involving over 100 individual email accounts.

The team at Avanan claims that they found an earlier exploit in Google Docs last June—one that allowed hackers to send phishing links to users. Then, this past October, they discovered that hackers had found another way to send phishing links to unsuspecting users, using the comment feature. They further claim that the vulnerability was not fixed by Google and because of that they began seeing hackers taking advantage of the vulnerability last month.

The hacking approach is both simple and straightforward—a hacker creates a Google Docs document and adds comments to it that include an @ symbol followed by an email address. The symbol automatically alerts the system to send an email to the person designated in the email address—the email that is sent has phishing links in it, sending the user to a webpage that could lead to malicious code.

The hack works because the email that is sent does not show the hackers' email address—just a name they designate. And because the email comes from Google, users trust that it is legitimate. The same feature also allows the email to sneak its way through spam filters. Notably, victims do not even have to open a Google Docs document to be targeted because they are targeted by what appears to be a friendly email message. To make matters worse, the attacker does not even have to share the document—just putting a victim's address in a comment gets the job done.

The team at Avanan reports that thus far, most attacks have involved Outlook but note it could work equally well for virtually any email system. They also note that to avoid falling victim to such an attack, users need only refrain from clicking on links embedded in emails sent from Google Docs. They close by claiming that they briefed Google on

their findings on January 4 but thus far the vulnerability has not been fixed.

More information: www.avanan.com/blog/google-doc … phishing-and-malware