

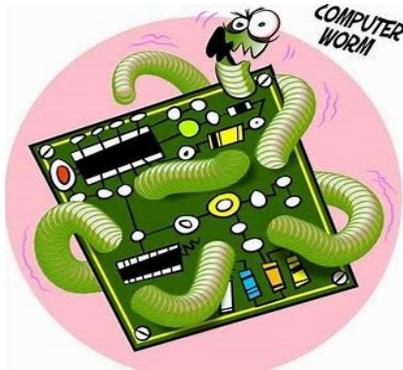


J622 Cybersecurity Policy Branch

Microsoft fixes wormlike account hijacking exploit in Teams

BY MARIA DEUTSCHER

Microsoft Corp. has updated its Microsoft Teams collaboration service to fix a security flaw that could have allowed hackers to hijack user accounts simply by posting a malicious image to a chat channel.



The vulnerability was originally spotted by publicly traded cybersecurity provider CyberArk Software Inc., which detailed its findings in a [report](#) today.

Microsoft Teams has an authentication mechanism that ensures users have permission to view images shared with them in a chat channel. After verifying that a person has access rights, the mechanism assigns them a unique authentication token. The problem is that this credential can be used for more than just viewing images.

CyberArk researcher Omer Tsarfati discovered that users' image-viewing tokens could be abused by a hacker to hijack their Microsoft Teams account. The vulnerability made it possible for hackers to read victims' messages, as well as send messages on their behalf to colleagues and thus compromise yet more people in their company.

"One of the biggest and the scariest things about this vulnerability is that it can be spread automatically, similar to a worm virus," Tsarfati wrote today.

To exploit the vulnerability, hackers would have first needed to gain access to a Microsoft Teams chat channel operated by the targeted company. A resourceful attacker could have accomplished that by compromising a poorly protected user account or by tricking a worker into sending an invite via means such as a phishing email, according to CyberArk.

Once inside, an attacker could have posted a GIF image file to the chat room with a malicious HTML attribute to hijack the image-viewing tokens of all the users who view the image. "When the victim opens this message, the victim's browser will try to load the image and this will send the authtoken cookie to the compromised sub-domain."

The catch is that the image can't send data to any subdomain but only to ones tied to Microsoft Teams servers, which complicates the attack. However, CyberArk found two vulnerable Microsoft Teams subdomains that were susceptible to takeover, which means it was possible to carry out the attack in practice before the release of the patch.

"Every account that could have been impacted by this vulnerability could also be a spreading point to all other company accounts," CyberArk's Tsarfati wrote. "The GIF could also be sent to groups (aka Teams), which makes it even easier for an attacker to get control over users faster and with fewer steps."

Retrieved on 4/27/2020 from <https://siliconangle.com/2020/04/27/microsoft-fixes-wormlike-account-hijacking-exploit-teams/>