Viewing GIFs can also be hacked for Microsoft Teams account

The outbreak of the COVID-19 pandemic led to a rapid increase in the number of Microsoft Teams users working remotely.

The outbreak of the COVID-19 pandemic led to a rapid increase in the number of Microsoft Teams users working remotely. However, this has also caused Teams to receive unwanted attention from cybercriminals.

Cyber ??security researchers from the CyberArk security team have recently found a vulnerability related to subdomain hijacking combined with malicious .GIF animations, which can be used by hackers. to "occupy valuable personal data in Microsoft Teams user accounts".

The team said that this relatively serious security flaw affects the Microsoft Teams platform on both desktop versions as well as on web browsers. What makes the vulnerability more dangerous lies in the value of data that hackers can steal if successfully hacked into a victim's account. The majority of Microsoft Teams' customers are businesses and organizations, so the platform currently contains a large amount of valuable information at the enterprise level - an attractive bait that cybercriminals target.

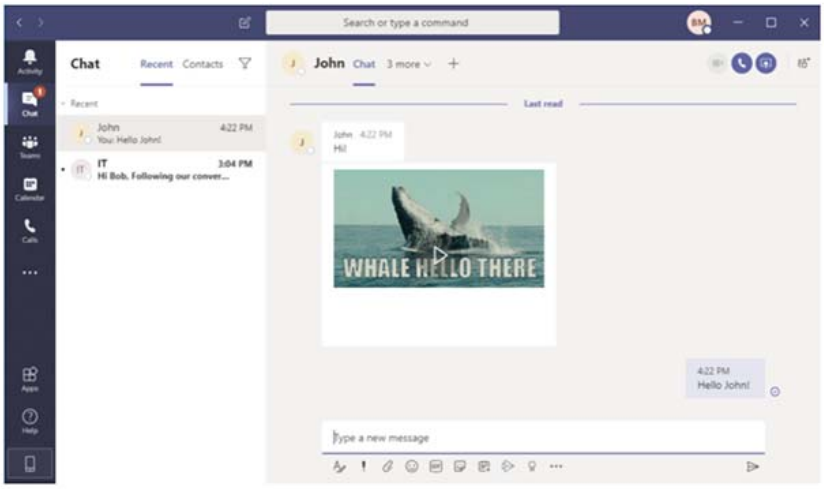
During the vulnerability detection process, the CyberArk team discovered that every time the application was opened, the Teams client automatically generated a new access token, authenticated via login. microsoftonline.com. Other similar tokens are created to access integrated support services like SharePoint and Outlook.

The 2 cookies used to restrict access to content are "authtoken" and "skypetoken_asm". The Skype token is sent to teams.microsoft.com and its subdomains - two of which were found to be vulnerable to hijacking.

"If an attacker could somehow force a user to gain access to the subdomains already taken, the victim's browser will send this cookie to the attacker's server and they can generate a Skype token. After doing all this, an attacker could steal the victim's Teams account data , " the CyberArk team said.

However, this chain of attacks is very complex, as an attacker needs to issue certificates for compromised subdomains - only possible by 'proving' ownership by tests like uploading a file. specific path.

To overcome this problem, the hacker will send malicious links to vulnerable subdomains, or .GIF files containing malicious tokens designed to hijack Teams users' session when they click on that .GIF file. This attack can affect multiple individuals at a time.



Malicious GIF file

All information about the flaw was reported by CyberArk to Microsoft, and the Redmond company has quickly released a patch to fix the vulnerability as well as minimize the risk of similar errors in the future.