Warning: Phishing attacks targeting Microsoft Teams show signs of sharp increase

Microsoft Teams is reluctant to be the new target that online scammers are targeting.

The outbreak of the COVID-19 pandemic has forced hundreds of millions of people to work, study at home, the need for online support platforms in general and video conferencing in particular. Because of that, it increased sharply. Microsoft Teams is a prime example, this remote support platform has achieved impressive growth growth in April, with the number of regular users increasing by 70% in just over 1 month.

However, this is also the reason why Microsoft Teams is reluctant to become the new target that online scammers are targeting.

According to the latest finding from the security organization Abnormal Security, the attackers started sending emails that impersonate automated notifications from Microsoft Teams to deceive users, then steal the victims' credentials. unaware.

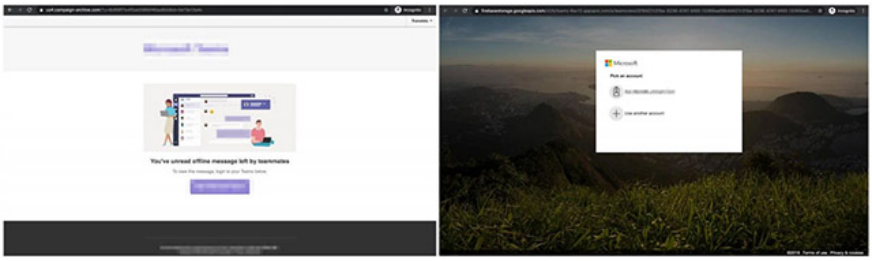
Fake emails are designed meticulously, with links leading to malicious landing pages that also look identical to Microsoft's legitimate website. In particular, attacks reported by Abnormal Security do not tend to target individuals or businesses in a specific field like many other phishing campaigns. Instead, malicious emails can be sent to anyone, making the infection rate harder to control.

Phishing email form

To evade malicious link detection tools and hide the real URL of the domain name being used to organize attacks, hackers use multiple URL redirects. There have been at least two separate phishing attacks targeting Microsoft Teams recorded by Abnormal Security in April alone.

In the first attack, phishing emails contained links to documents stored on a website used by an email marketing company. This document contains 1 image that requires users to log in to their Teams account. When clicking on the image, the victim will be redirected to the fake landing page of Microsoft Office account login page to steal login information.

In the second campaign, the link in the email redirects the user to a page on YouTube and then redirects a few more times before reaching the landing page stealing credentials. Because Microsoft Teams is linked to Microsoft Office 365, an attacker may have access to other data associated with the victim's Microsoft login information through a single sign-in.



The fake Office 365 login page
These two campaigns are most likely not of the same origin. They have different payload distribution content and methods. At the same time using the sender information is not the same.

A few days ago, another serious flaw was discovered on Microsoft Teams, allowing hackers to hijack user accounts with just a GIF file.

In general, this form of fraud has been designed more sophisticatedly but it is not new in nature. Even so, it will still be dangerous for ordinary users who do not have a lot of security knowledge.