Beware of these Microsoft Teams scams!

As one of the most popular collaboration tools worldwide, there are millions of potential victims of Microsoft Teams scams — but there are some helpful ways to spot these scams.

Hackers are using Microsoft Teams to launch phishing, vishing, and quishing campaigns, using social engineering to trick victims into sharing sensitive private data. As one of the most popular collaboration tools in the world, there are millions of potential victims of Microsoft Teams scams – but there are some helpful ways to spot them.

MFA Authentication Scam

Believed to be from the same group behind the SolarWinds attack, this scam bypasses multi-factor authentication using social engineering tactics. The attackers use previously compromised Microsoft 365 tenants to create a new security-themed "onmicrosoft.com" subdomain and add a new user. The attackers also rename the tenant to "Microsoft Identity Protection" or something similar.

Next, they send the target a chat request. If the user accepts, they send them an MS Teams message with a code, which they are then persuaded to enter into the Microsoft Authenticator app on their device. Once the target enters the code into the authenticator app, the hacker gains access to the target's Microsoft 365 account. The attacker can then steal information from the MS 365 tenant or add a managed device to the organization.

Black Basta Ransomware Attack

The infamous Black Blasta ransomware group also targeted Microsoft Teams logins, using a social engineering campaign to bombard email addresses with spam. Hackers contacted MS Teams users pretending to be the company's IT support or help desk, offering to fix an ongoing spam problem, which often included non-malicious emails like subscription confirmations, newsletters, or email verifications to flood users' inboxes.

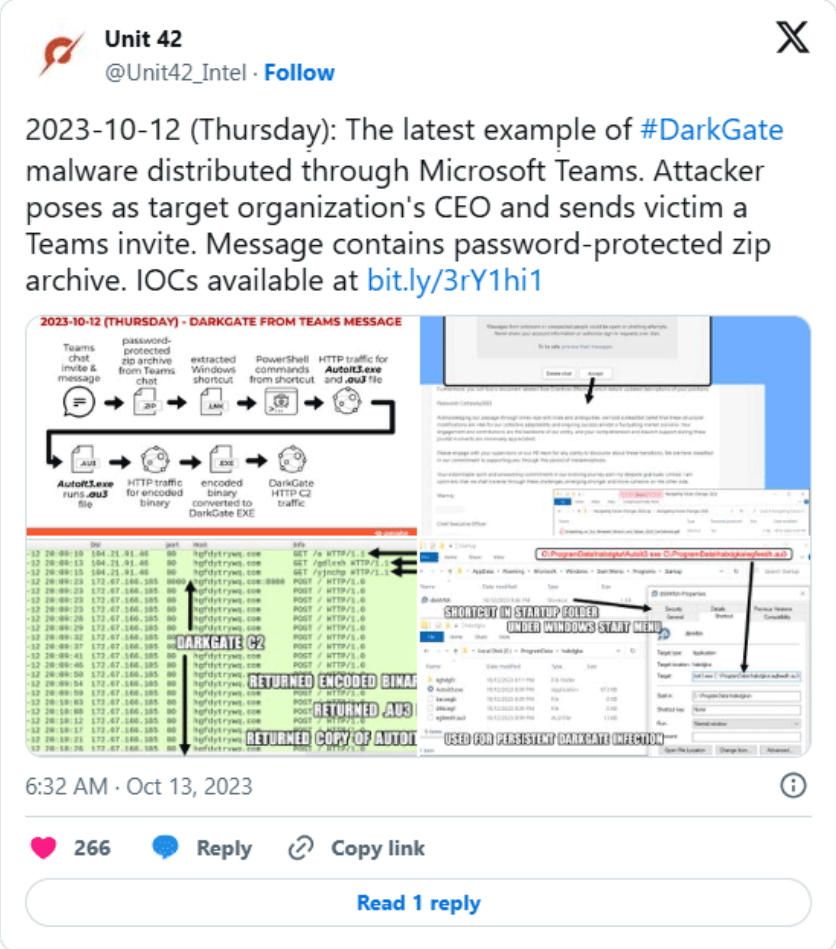
Next, the hackers call the overworked employee and try to get them to install a remote desktop access tool, where they can take control of the user's machine. Once they have control, they can install a variety of malware, including remote access Trojans (RATs), Cobalt Strike, DarkGate malware, and other dangerous software. Ultimately, Black Blasta gains complete control of the machine and can steal as much data from the network as possible.

Fake Microsoft Teams Job Scam

Fake job scams have been around for a while, targeting job seekers, and scammers are using Microsoft Teams chat to exploit their victims. An attacker emails you about a fake job and suggests using Microsoft Teams to conduct the interview. Here's the first red flag: The entire interview will be conducted over chat.

You will then be offered a fake job and asked to submit your information to the company's database. Some victims receive a Google Doc form asking for their PII and social security/tax numbers. In some cases, victims are asked to purchase items to perform the job, pay a recruitment fee, or purchase gift cards, some of the most common signs that a job offer is questionable.

Fake Microsoft Teams HR using malicious ZIP file



Attackers not only impersonated IT support teams, but also HR staff. The attack, first detected in 2023, began with messages from someone posing as an HR employee using a previously compromised Microsoft 365 account. In some cases, the attacker even posed as a company executive.

The target receives a phishing message explaining that there will be changes to the employee leave schedule and that several people, including the victim, will be affected. The phishing message contains a download link for the new schedule, which is actually a link to the DarkGate malware. If the malicious file is executed on the target machine, it installs the malware, giving the attacker full access to the device and its data.

Malicious PDF file sent via Microsoft Teams

Attackers also used compromised Microsoft 365 accounts to send malicious executables disguised as PDF files. This attack starts with a Microsoft Teams chat invitation that, if accepted, actually downloads a seemingly harmless PDF file. However, it's actually a malicious executable that uses a double extension to trick you. So the extension looks like PDF, but it's actually an EXE.

The file is usually named something that requires immediate action, such as "Navigating Future Changes.pdf.msi", which when opened, will actually download malware.

How to protect yourself

You should always be cautious with external messages and invitations you receive on Microsoft Teams. Even if they appear to be from someone else, it's best to double-check, especially if they involve files, links, or chat invitations that you weren't expecting to receive. Never give control of your device to a third party unless you've verified that it's from a legitimate representative of your IT team. Be wary of urgent calls to action in emails and messages, as they're often designed to get you to act before you've thought it through.

Other ways to protect yourself from phishing scams include using link checker sites to determine if a link is safe or domain age checker sites that allow you to see the exact age of a domain. Malicious phishing sites are often only live for a few days, weeks, or months and often mimic addresses to try to fool you.